MCWP 2-14

Counterintelligence

U.S. Marine Corps

5 September 2000

PCN 143 000084 00

To Our Readers

Changes: Readers of this publication are encouraged to submit suggestions and changes that will improve it. Recommendations may be sent directly to Commanding General, Marine Corps Combat Development Command, Doctrine Division (C 42), 3300 Russell Road, Suite 318A, Quantico, VA 22134-5021 or by fax to 703-784-2917 (DSN 278-2917) or by E-mail to **morgannc@mccdc.usmc.mil**. Recommendations should include the following information:

- Location of change
  - Publication number and title
  - Current page number
  - Paragraph number (if applicable)
  - Line number
  - Figure or table number (if applicable)
- Nature of change
  - Add, delete
  - Proposed new text, preferably double-spaced and typewritten
- Justification and/or source of change

Additional copies: A printed copy of this publication may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status.* An electronic copy may be obtained from the Doctrine Division, MCCDC, world wide web home page which is found at the following universal reference locator: **http://www.doctrine.usmc.mil**.

Unless otherwise stated, whenever the masculine gender is used, both men and women are included.

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, D.C. 20380-1775

5 September 2000

FOREWORD

Marine Corps Doctrinal Publication (MCDP) 2, *Intelligence*, and Marine Corps Warfighting Publication (MCWP) 2-1, *Intelligence Operations*, provide the doctrine and higher order tactics, techniques, and procedures for intelligence operations. MCWP 2-14, *Counterintelligence*, complements and expands on this information by detailing doctrine, tactics, techniques, and procedures for the conduct of counterintelligence (CI) operations in support of the Marine air-ground task force (MAGTF). The primary target audience of this publication is intelligence personnel responsible for the planning and execution of CI operations. Commanders, planners, and other personnel who use the results from CI operations or provide support to them should also read this publication.

MCWP 2-14 describes aspects of CI operations across the spectrum of MAGTF, naval, joint and multinational operations, including doctrinal fundamentals, equipment, command and control, communications and information systems support, planning, execution, security, and training. MCWP 2-14 provides the information needed by Marines to understand, plan, and execute CI operations in support of the MAGTF across the spectrum of conflict.

MCWP 2-14 supersedes FMFM 3-25, *Counterintelligence*, dated 22 September 1992.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

B. B. KNUTSON, JR.
Lieutenant General, U.S. Marine Corps
Commanding General
Marine Corps Combat Development Command

DISTRIBUTION: 14300008400

COUNTERINTELLIGENCE

Table of Contents

Chapter 7. Execution of CI Activities

Chapter 10. Garrison Counterintelligence Support

Appendices

CHAPTER 1. DOCTRINAL FUNDAMENTALS

Intelligence strives to accomplish two objectives. First, it provides accurate, timely, and relevant knowledge about the enemy (or potential enemy) and the surrounding environment. The primary objective of intelligence is to support decisionmaking by reducing uncertainty about the hostile situation to a reasonable level, recognizing that the fog of war renders anything close to absolute certainty impossible. The second intelligence objective assists in protecting friendly forces through counterintelligence (CI). CI includes active and passive measures intended to deny the enemy valuable information about the friendly situation. CI includes activities related to countering hostile espionage, subversion, and terrorism. CI directly supports force protection operations by helping the commander deny intelligence to the enemy and plan appropriate security measures. The two intelligence objectives demonstrate that intelligence possesses positive—or exploitative—and protective elements. It uncovers conditions that can be exploited and simultaneously provides warning of enemy actions. Thus, intelligence provides the basis for our own actions, both offensive and defensive. Identifying, planning, and implementing MAGTF operations and measures are the main focus of this publication.

1001. OBJECTIVE

CI—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (Joint Publication [JP] 1-02)

The principal objective of CI is to assist with protecting friendly forces. CI is the intelligence function concerned with identifying and counteracting the threat posed by hostile intelligence capabilities and by organizations or individuals engaged in espionage, sabotage, subversion or terrorism. CI enhances command security by denying an adversary information that might be used to conduct effective operations against friendly forces and to protect the command by identifying and neutralizing espionage, sabotage, subversion or terrorism efforts. CI provides critical intelligence support to command force protection efforts by helping identify potential threats, threat capabilities, and planned intentions to friendly operations while helping deceive the adversary as to friendly capabilities, vulnerabilities, and intentions. Physical security reduces vulnerability. Operations security reduces exposure. Combating terrorism makes us a less lucrative target. CI increases uncertainty for the enemy, thereby making a significant contribution to the success of friendly operations. CI also identifies friendly vulnerabilities, evaluates security measures, and assists with implementing appropriate security plans. The integration of intelligence, CI, and operations culminates in a cohesive unit force protection program.

1002. BASIC CONSIDERATIONS FOR CI ACTIVITIES

Hostile Objectives

Adversaries can be expected to use every available means to impede our forces with their efforts directed towards intelligence, espionage, sabotage, subversion, and terrorist operations. Hostile intelligence collection activities are directed toward obtaining detailed knowledge of our forces and their

capabilities, limitations, centers of gravity, vulnerabilities, intentions, and probable courses of action. These activities also obtain information concerning the area of operations including weather, terrain, and hydrography.

Adversarial Advantage

Adversary knowledge of friendly operations concentrates efforts on preparing the objective for defense, attacking friendly staging areas, and disrupting the operation through espionage, sabotage, terrorism, and subversive activities. CI is essential to the security of our forces—commencing with routine garrison operations, to the inception of planning, and until the operation is complete—to deny the enemy advantage and manipulate understanding us.

Hostile Espionage Activities

Foreign intelligence services (FIS) capabilities must be accurately assessed. FIS should be assumed to be at least as effective as our own. An adversary should always be given the benefit of the doubt in collecting information and producing intelligence on friendly operations. FIS do not normally develop vital intelligence by obtaining one all-revealing fact. Most worthwhile intelligence is the product of the assembly, comparison, and interpretation of many small and seemingly insignificant items of information.

Enemy Sabotage Activities

Sabotage is an act or acts with intent to injure, interfere with or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities including human and natural resources. Immediately prior to the outbreak of hostilities, during combat, and even during military operations other than war (MOOTW), the enemy can be expected to employ sabotage techniques to disrupt friendly operations.

Subversive Activities

Subversive activities are designed and conducted to undermine the authority of friendly forces and/or that of the local government to disrupt friendly activities or to gain aid, comfort, and moral support for the cause of the enemy or hostile force or group. Subversive activity can be directed against individuals, groups, organizations or entire populations. Frequently, subversive activity supports, conceals or provides a favorable environment for espionage, sabotage, and terrorist operations. Subversion is an action designed to undermine the military, economic, psychological, political strength or morale of a regime.

Terrorist Activities

Any personality, organization or installation of political or military significance could be a terrorist target. Terrorists have become adept in the calculated and systematic use or threat of violence in pursuit of their political or ideological goals. Although the tactics and methods of operation of terrorists may vary from group to group, the techniques they employ to dramatize their goals through fear, intimidation, and coercion are similar.

1003. CONCEPTS OF CI AND FORCE PROTECTION

Security—Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (JP 1-02)

Historical Services Perspectives

The CI agencies within the four Services have historically demonstrated dramatically different CI areas of emphasis, concepts of operations, and methods of execution.

Naval Criminal Investigative Service and Air Force Office of Special Investigations

The Naval Criminal Investigative Service (NCIS) and the Office of Special Investigations (OSI) have traditionally viewed CI with a strategic focus drawn from their perspectives as, primarily, law enforcement organizations. NCIS is mainly a civilian investigative organization with a chain of command directly from the Secretary of the Navy to the Director, NCIS. The Director, NCIS, has exclusive responsibility for CI policy development and implementation and execution and management of CI programs, with the exception of those combat and combat related CI responsibilities of the Marine Corps. CI activities of NCIS are funded from the Foreign Counterintelligence Program (FCIP). OSI is a field-operating agency of the Air Force. Policy and programmatic oversight rests with the Secretary of the Air Force Office of the Inspector General, not the Director of Intelligence. CI activities of OSI are also funded from the FCIP. Like NCIS, there is no programmatic provision in OSI for tactical intelligence and related activities (TIARA) funding or resources.

Marine Corps and the Army

The Army and Marine Corps maintain CI as a component of their intelligence staffs. The Marine Corps CI orientation is entirely tactical, with funding exclusively within the DON's budget for TIARA. The Army emphasizes both strategic and tactical CI and is supported by a mixture of FCIP and TIARA resources.

Joint

During the development of joint CI doctrine, the issue arose whether CI should fall under the staff cognizance of intelligence or operations because of differences in emphasis and support for CI. Doctrinal evolution has placed the CI of the combatant commands and joint task forces (JTF) command under the joint intelligence staff (J2).

Joint Operations and CI

Exercising command and control of CI assets vary under different circumstances. Military department CI elements are under the command and control of their respective department secretaries to carry out their statutory authorities and responsibilities. However, combatant commanders may choose to exercise staff coordination authority over military department CI elements deployed within their area of responsibility. Staff coordination authority is intended to encompass deconfliction of CI activities and assurance of unity of effort in attaining the military department secretaries' and combatant commanders' CI objectives. If a military operation plan or

operation order so specifies, a combatant commander or JTF commander may, on National Command Authority-directed execution, assume operational control of military department CI elements assigned to support the operation for the duration of the operation, including predeployment, deployment, and redeployment phases. Under this authority, Service CI elements are under the combatant commander's authority. MAGTF CI elements, however, are under the operational control of the MAGTF unless otherwise specified. Law enforcement and CI investigations and attendant matters carried out by CI elements remains solely a military department's administrative responsibility.

CI and Intelligence

CI, like intelligence matters, is a command responsibility. In preparing for operations, units must develop a CI plan and implement appropriate CI measures to protect themselves from potential threats. CI is integrated into the overall intelligence effort to identify and counter an adversary's intelligence efforts. Failure to adequately plan for and implement CI operations and measures may result in serious damage to the MAGTF or supported unit. Continuing attention to CI and effective intelligence and operations integration is thus required at all levels of command, from the MAGTF commander to the individual Marine.

CI and Force Protection

Force protection—A security program designed to protect soldiers, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, personal protective services, and supported by intelligence, CI, and other security programs. (JP 1-02)

Force protection is a responsibility of command. An operations function, force protection is under the staff cognizance of the unit operations officer. CI is a significant contributor to the command's overall force protection effort. Security is a matter of vulnerability and threat assessment with effective risk management. CI helps identify the hostile intelligence threat, assists in determining friendly vulnerabilities to it, and aids with the development of friendly measures that can lessen or negate these. The commander weighs the importance of intelligence and CI to be used as a tool in risk management. Marine Corps CI elements provide unique force protection capabilities through both active and passive CI measures and human resource intelligence (HUMINT) support. Often, CI elements can provide unique intelligence support to the commander's estimate of the situation and situation development (e.g., providing an assessment of the mood of the area of operations, allowing us to feel the pulse of an incident as it develops). CI also provides critical support to the command's overall intelligence efforts by providing indications and warning (I&W) of potential attack and support to targeting and combat assessment efforts.

1004. MAGTF CI OPERATIONS

Responsibilities

The unit intelligence officer plans, implements, and supervises the CI effort for the commander. The G-2/S-2 may have access to or request support from MAGTF CI units and specialists to assist in developing CI estimates and

plans. Members of the command are involved in executing the CI plan and implementing appropriate CI measures. Key participants in this process and their specific responsibilities are—

- Unit security manager (generally the chief of staff or executive officer, but often the unit's intelligence officer)—overall integration and effectiveness of unit security practices.
- G-3/S-3—force protection, operations security (OPSEC), counterreconnaissance, and deception.
- G-6/S-6—communications and information systems security.
- G-1/S-1—information and personnel security.
- Headquarters commandant—physical security of unit command post and echelons.

CI Process

The CI process at all levels is conducted by using a standard methodology that consists of four steps: develop a CI estimate, conduct CI survey(s), develop the CI plan, and conduct CI operations and assist with implementation of CI measures. Figure 1-1 summarizes the CI process.

The CI Estimate

Included in CI estimates are known factors on location, disposition, composition, strength, activities, capabilities, weaknesses, and other pertinent information. CI estimates also provide conclusions concerning probable courses of action and future activities of these organizations, effects of those activities on friendly courses of action, and effectiveness of friendly force CI measures. Comprehensive CI estimates are normally prepared by senior echelon commands. Within the MAGTF, intelligence and CI analysts of the MAGTF CE, intelligence battalion (intel bn), and its CI/HUMINT company/detachment will normally prepare a tailored CI estimate that addresses threats to the MAGTF by using an IPB methodology that is focused on CI factors and the CI threat. However, each level of command must conduct its own evaluation to determine which adversary's capabilities identified in the MAGTF CI estimate represent a threat to their particular unit. The CI estimate must be updated on a regular basis, and the revised

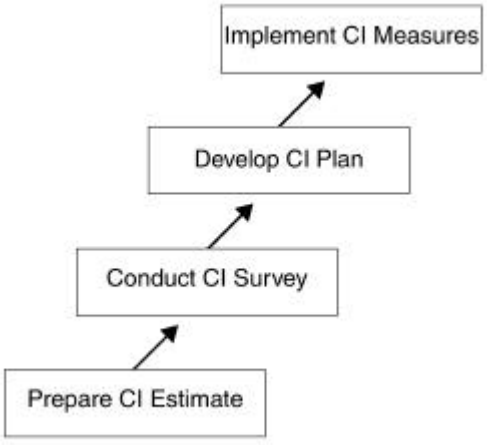

Figure 1-1. The CI Process.

CI estimates provide information on enemy intelligence, sabotage, subversive, and terrorist organizations relevant to the current mission, situation and area of operations.

estimate or appropriate CI warning reports must be disseminated to units involved in the operation.

The CI Survey

The CI survey assesses a unit's security posture against the threats detailed in the CI estimate. The CI survey should identify vulnerabilities to specific hostile intelligence, espionage, sabotage, subversion or terrorist capabilities and provide recommendations on how to eliminate or minimize these vulnerabilities. The survey should be as detailed as possible. During the planning phase of an operation, it may be possible to do a formal, written survey. In a time-compressed situation, the survey will likely result from a brief discussion between the appropriate intelligence, CI, operations, communications, and security personnel. It is critical that the survey look forward in both space and time to support the development of the CI measures necessary to protect the unit as it carries out successive phases of the operation; the survey makes recommendations to improve the CI posture of the command both now and in the future.

The CI Plan

The CI plan details the activities and operations that the command uses to counter hostile intelligence, sabotage, subversion, and terrorist threats. It includes procedures for detecting and monitoring the activities of hostile intelligence and terrorist organizations and directs the implementation of active and passive measures that are intended to protect the force from these activities. The CI plan is based on the threats identified in the CI estimate and the vulnerabilities detected by the CI survey. The intel bn commander, as the intelligence support coordinator (ISC), assisted by CI/HUMINT company, the production and analysis (P&A) cell officer in charge (OIC), and the MEF staff CI officer, will normally prepare a detailed, comprehensive CI plan that addresses the MEF and is integrated with CI plans of the JTF and other pertinent forces. Included in the MAGTF CI plan are details of the employment of dedicated CI capabilities and the conduct of specialized CI operations intended to detect and neutralize or eliminate specific threats. Plans of subordinate MAGTF elements closely follow the MAGTF plan, normally adding only security measures that are applicable to their specific units.

As with all plans, CI plans must be continually updated to ensure they are current and support both ongoing and future operations.

CI Execution

One of the most highly effective tools of the CI collection activity is the counterintelligence force protection source operations (CFSO).

An understanding of the interest and capability of adversarial intelligence organizations to collect information on evolving U.S. technologies is critical to developing appropriate countermeasures. CI personnel can readily obtain information from other national intelligence and security organizations because of its unique liaison arrangements. That capability not only supports the analytical efforts of the national agencies and intelligence centers, but also give an added dimension to I&W. The CFSO provides commanders with a collection and production capability to protect their forces without resorting to complex national coordination procedures. The role of CI is even greater as U.S. military operations increasingly rely upon cooperation and support of our allies. CI personnel can assess the capabilities, effectiveness, organization, and methods of operation of allied intelligence

services as well as the effectiveness of their security procedures and ability to support or to detract from the U.S. effort.

1005. CI MEASURES

CI measures—both active and passive—encompass a range of activities designed to protect against hostile intelligence, espionage, sabotage, subversion, and terrorism threats.

CI analysis develops threat assessments that assist decisionmakers in determining the threat posed to their plans, strategies, resources, programs, operations and systems by foreign intelligence activity.

Active Measures

Active CI measures are those designed to neutralize the multi-discipline intelligence effort (all disciplines used to collect intelligence such as HUMINT, signals intelligence [SIGINT], and imagery intelligence [IMINT]) and hostile efforts toward sabotage, subversion, and terrorism. Active CI measures include counterespionage, countersabotage, countersubversion, counterterrorism, counterreconnaissance, concealment, and deception operations and vary with the mission and capabilities of the unit.

Passive Measures

Passive CI measures are designed to conceal and deny information to the enemy, protect personnel from subversion and terrorism, and protect installations and material against sabotage. Measures include security of classified material, personnel security, physical security, security education, communications security, data security, electromagnetic emission security, censorship, camouflage, concealment, light, and security discipline. Passive measures are readily standardized in the unit's standing operating procedures (SOPs) regardless of the unit's mission.

Types of CI Measures

The three general CI measures are denial, detection, and deception. Frequently, the measures applied to accomplish one of these purposes contribute to the others.

Denial Measures

Denial measures are applied to prevent the enemy from gaining access to classified and sensitive information, subverting personnel, and penetrating the physical security barriers established at command posts and echelons, facilities, and installations. Counterreconnaissance is one example of a denial measure that may be used.

Detection Measures

Detection measures are used to expose and to neutralize enemy efforts directed toward intelligence collection, sabotage, subversion, and terrorism. MAGTF units detect or aid in the detection of these enemy efforts by collecting, analyzing, and reporting information on enemy activities that may indicate an intelligence effort by establishing checkpoints to control the

movement of personnel within or through their areas of responsibility and by evacuations of possible enemy agents and materials to higher echelons for interrogation and exploitation. Other detection measures, usually accomplished by specialists, include document translation and analysis, screening, interrogation, and offensive and defensive CI activities.

Deception Measures

Control of deception operations should be at the highest level of command likely to be significantly affected by the enemy's reactions.

Deception measures mislead or otherwise confuse the enemy concerning our capabilities, centers of gravity, vulnerabilities, plans, and intentions. Deception measures may include feints, ruses, demonstrations, and the provision of false information to the enemy. Deception measures depend on effective command security for success. Special precautions must be taken ensuring there is no leakage of friendly force information during the planning or execution of an operation. When enemy intelligence activities are identified, consideration must be given to the potential for using that activity in support of deception measures. The potential threat posed by the enemy must be weighed against the potential intelligence benefits of continued exploitation of the enemy's intelligence system versus its destruction or other degradation

1006. CI SUPPORT TO OPERATIONS

MAGTF CI support to operations normally falls within one of the following two categories: support to military security or civil security.

Support to Military Security

Military security encompasses all measures taken by a command to protect itself from sabotage, terrorism, and subversion and to deny information to the enemy. MAGTF units emphasize protection of airfields and other major installations and the defeat of hostile target acquisition efforts. Typical measures include OPSEC, counterreconnaissance, countersigns, passwords, and restrictions on access to selected areas and installations.

Support to Operations Security

OPSEC is the functional responsibility of the operations officer (G-3/S-3).

To be effective, OPSEC vulnerabilities must be determined and countermeasures implemented commencing with operational planning and continuing through completion of any operation. Commanders must determine what essential elements of friendly information (EEFI) and operations must be protected, what OPSEC measures to implement, when to implement them, and what level of risk they are willing to accept. Commanders, staffs, and individuals at all echelons of command are responsible for developing and implementing an effective OPSEC program.

OPSEC denies the enemy prior knowledge of EEFI regarding command activities, plans, operations, strengths, vulnerabilities, and intentions. The enemy collects this information through a variety of means—human, electronic, photographic, etc. To effectively counter this threat, commanders must have access to timely, reliable, and accurate intelligence on enemy intelligence capabilities and operations.

Support to Information Security and C2 Protect

CI supports commanders' OPSEC programs by providing assessments of friendly vulnerabilities; briefings on enemy threats of espionage, sabotage, subversion, and terrorism; and assistance in establishing safeguards and countermeasures against these threats.

The INFOSEC program—a responsibility of the unit's security manager—includes a proper security classification determination being made with applicable security regulations and the proper protection being afforded to the material throughout its life cycle. These measures include proper preparation, reproduction or manufacturing, storage, use, and destruction. Failure to comply with required INFOSEC measures exposes sensitive information to potential compromise. The rapid advancement of the microprocessor and the maturity of computer age technologies have presented a significant new area of exposure that leaves us particularly vulnerable. While these advances provide new capabilities and opportunities, they also create new vulnerabilities to be exploited. Evolving information operations (IO) concepts and doctrine recognizes the potential and the threats created by this trend. IO include actions taken to affect adversary information while defending one's own information and information systems during both routine peacetime, MOOTW, and combat operations. Command and control protect are defensive measures taken to detect and prevent hostile efforts against our C2 and supporting communications and information systems. The ability to directly influence key decisionmakers through the injection, disruption, manipulation or destruction of information and information means is a powerful tool in the advance of military objectives. Information system vulnerabilities include denial of service, information theft, information replacement or introduction of false data. Defensive measures to provide information assurance include use of secure networks, firewalls, encryption, anti-virus scans to detect malicious code, and proper systems administration to include aggressive auditing. Information protection includes the authenticity, confidentiality, availability, integrity, and non-repudiation of information being handled by anyone involved with C2. It requires proper implementation of appropriate security features such as passwords, authentication or other countermeasures. The criticality for CI in this area is the ability to identify the adversary's potential capability to exploit, deny, degrade or destroy friendly C2 before an attack to counter the attempt. Reporting and tracking of attempted and successful attacks will, through trend analysis, assist in the development of countermeasures.

Information security (INFOSEC) is designed to protect sensitive information from potential unauthorized release or compromise.

Counterreconnaissance

Units may be assigned both reconnaissance and counterreconnaissance responsibilities; these two activities complement each other and are inseparable. Good reconnaissance ensures a certain amount of security, and counterreconnaissance provides a certain amount of reconnaissance information. However, a unit tasked with a reconnaissance mission is not ordinarily given a supplementary counterreconnaissance mission as completing the counterreconnaissance mission generally requires neutralizing the hostile reconnaissance elements, while the primary goal of reconnaissance is collection of information without being detected by the enemy. Counterreconnaissance includes setting up a defensive screen to deny enemy reconnaissance or an offensive screen designed to meet and destroy enemy reconnaissance in combat air operations. Counterair operations may be defined as counterreconnaissance when counterair

operations deny or reduce an enemy's capability for visual, photographic or electromagnetic reconnaissance.

One of the most effective CI measures taken by a unit is counterreconnaissance.

Principles of Counterreconnaissance. Counterreconnaissance elements focus on friendly forces being screened. Hostile reconnaissance forces are destroyed or neutralized, and friendly screening forces are echeloned in depth.

Forms of Counterreconnaissance. The defensive screen is protective. It is usually established behind natural obstacles. An offensive screen may be moving or stationary depending on the activities of the friendly force being screened. The offensive screen meets the enemy's reconnaissance forces and neutralizes them. The commander's adoption of a form of counterreconnaissance screen depends on the situation, mission, weather, and terrain; thus the form of counterreconnaissance screen adopted, need not reflect solely the tactical mission of the command. Because there are offensive and defensive screens does not imply a requirement for their employment only in support of a like tactical mission. An offensive screen may well be employed to support a tactical mission of defense, while an attack mission may be supported best by a defensive screen.

Support to Embarkation Security

Embarkation security consists of the special application of military and civil security measures to the embarkation phase that include the movement to the point of embarkation and the actual embarkation. Examples include the screening of civilians employed in the port or airfield, control of contact between troops and civilians, covering or removing tactical markings and other unit designations, and moving to the port or airfield under the cover of darkness.

Support to Civil Security

Civil security operations are generally conducted in coordination with law enforcement, civil affairs, and other appropriate agencies.

Civil security operations include CI measures affecting the civilian population of the area. Typical measures include security screening of civilian labor, imposing curfews and other circulation control measures, and the monitoring of suspect political groups.

CHAPTER 2. COUNTERINTELLIGENCE FUNCTIONS AND SERVICES

2001. COUNTERINTELLIGENCE FUNCTIONS

There are four CI functions: operations; investigations; collection and reporting; and analysis, production, and dissemination (see table 2-1).

CI Operations

Offensive CI operations are the employment of specialized CI techniques and procedures. They are directed against the espionage, sabotage, subversive, and terrorism threat. These operations are planned, coordinated, and conducted by MAGTF CI personnel and include the following operations:

Counterespionage Operations

These operations are designed to detect, destroy, neutralize, exploit or prevent espionage activity. This is accomplished through the identification, penetration, manipulation, deception, and repression of individuals, groups or organizations conducting or suspected of conducting espionage activities.

Countersubversion Operations

These operations are designed to detect, prevent or neutralize the activities of subversive groups. Subversive activity is closely related to and frequently supports, conceals or provides a favorable environment for espionage and sabotage operations. Based on this environment, the countersubversive mission may include offensive measures directed toward the origin of hostile subversive plans and policies.

"...Mogadishu has been one tough nut to crack . . . we are making steady and perceptible progress. From my perspective, one of the most encouraging outgrowths of our efforts in this socially, politically and geographically complex urban environment has been the emergence of tactical HUMINT as the driving force behind operations . . . in-by-9 out-by-5 service on priority intelligence requirements."

". . . been directed against clearly defined targets—there have been remarkably few dry holes. Spared the long unproductive walks in the sun sometimes associated with the Vietnam Conflict. The troops have remained alert, tactically disciplined and tightly focused. I believe this accounts, in some measure, for our low casualty rate."

". . . it's refreshing to see things in their proper order—INTELLIGENCE DRIVING OPERATIONS . . . instead of operations driving intelligence."

—MajGen Charles E. Wilhelm
Commander, Marine Corps Forces Somalia

Table 2-1. Objectives of CI Functions.

CI Function	Objectives
CI Operations	Determine foreign intentions. Support tactical and strategic perception management operations. Support all-source intelligence and other CI operations. Support planning and military operations.
CI Investigations	Detect, exploit, prevent, or neutralize espionage activities. Detect and resolve incidents of foreign directed sabotage, subversion, sedition, terrorist activities, and assassinations. Document elements of proof for prosecutions. Provide military commanders and policy makers with intelligence and information to use to eliminate security vulnerabilities and improve security postures.
CI Collections and Reporting	Provide indications and warning of security threats to U.S. forces, facilities, and operations. Provide intelligence on threats to forces to support planning and implementation of defensive or offensive countermeasures. Respond to commander's priority intelligence requirements.
CI Analysis, Production, and Dissemination	Provide analysis and assessments of threats to U.S. forces, facilities, and operations. Provide causal analysis of past events to identify vulnerabilities and risks. Identify adversary organizations, personalities, and capabilities posing threats to forces, facilities, and operations.

Countersabotage Operations

These operations require a comprehensive program to penetrate saboteur, partisan or other dissident groups. The goal of the program is to determine sabotage plans and to identify saboteurs, methods of operation, and specific targets, and thus support MAGTF force protection efforts.

Counterterrorism Operations

These operations are planned, coordinated, and conducted to detect, prevent, or neutralize terrorist groups or organizations by determining terrorist plans or intentions. They are also employed to identify terrorists, methods of operation, and specific targets.

Exploitation and Neutralization Operations

These operations are targeted against personalities, organizations, and installations of intelligence or CI interest, which must be seized, exploited or protected. Screening and interrogations are operations designed to identify and apprehend enemy intelligence agents, subversives, terrorists, and saboteurs who attempt to infiltrate friendly lines and operations or conceal themselves among the civilian population.

CI Investigations

CI investigations are investigations concerning personnel, security matters, espionage, sabotage, terrorism, and subversive activities, including defection. A CI investigation is a duly authorized, systematic, detailed examination/inquiry to uncover and report the facts of a matter. Jurisdiction for CI investigations will vary according to which commander is exercising C2 of the force's CI assets. However, CI investigations and attendant matters carried out by a CI element remain part of the administrative responsibilities of the military department to which the specific CI element is subordinate.

Additionally, MAGTF CI elements may conduct investigations of friendly prisoners of war and persons missing (non-hostile) in action cases. The type of activities required in these investigations include collecting information of potential intelligence value on friendly personnel possibly in enemy hands (including debriefings of returned POW/MIA, with emphasis on identifying, locating, and recovering additional personnel) and the collection of information that aids in identifying, locating, and recovering those friendly personnel known or suspected in enemy hands. Initial damage assessments relating to the possible compromise of operational and sensitive material must be included.

CI Collections and Reporting

CI collections and reporting are a significant force multiplier, which are intended to identify actual and potential threats to the command. Collections include the following.

Liaison

Coordination (within authorized jurisdictional limitations) is conducted by CI elements with local intelligence, CI, security and law enforcement

organizations/agencies, and civil affairs and psychological operations units where appropriate. Within the DON, NCIS is the element exclusively assigned to maintain liaison with federal law enforcement, security and intelligence agencies on criminal investigative, CI and security matters. NCIS is the primary agency for liaison in these matters with state local and foreign law enforcement, security and intelligence agencies, including those of foreign and U.S. military departments. Following notification of the local NCIS office, MAGTF CI personnel may conduct liaison necessary to accomplish its mission during combat operations. If prior notification of NCIS is not possible, notification will be made at the earliest opportunity.

CI Force Protection Source Operations

CI force protection source operations (CFSO) are overt source collection activities of an expedient nature intended to identify threats to the command in support of the commander's force protection mission.

CI Analysis and Production

Limited initial analysis is conducted by MAGTF CI elements that originally collect and report the information. Detailed analysis occurs as part of the MAGTF's all-source intelligence effort.

2002. COUNTERINTELLIGENCE SERVICES

They enhance the security of the command against espionage, sabotage, subversion, and terrorism. Technical surveillance countermeasures (TSCM) involve the employment of services and techniques designed to locate, identify, and neutralize the effectiveness of hostile technical surveillance activity (see chapter 10).

CI services include CI surveys and vulnerability assessments, evaluations, inspections, training, and technical services.

2003. CI SUPPORT TO THE STRATEGIC, OPERATIONAL, AND TACTICAL LEVELS OF WAR

The levels of war form a hierarchy. Tactical engagements are components of battle, and battles are elements of a campaign. The campaign is but one phase of a strategic design for gaining the objectives of policy. While a clear hierarchy exists, there are no sharp boundaries between levels; they merge and form a continuum. A particular command echelon is not necessarily concerned with only one level of war. A commander's responsibilities within the hierarchy depend on the scale and nature of the operation and may shift up or down as the operation develops (see MCDP 1-1, *Strategy*, and MCDP 1-2, *Campaigning*, for additional information on the levels of war).

CI provides critical support to all three levels of war (see figure 2-1 on page 2-4). While certain activities may crosslevels based on the environment and the nature of the threat; the levels and type of CI support remain fairly distinct. The distinctions are based on the supported commander's intelligence and CI requirements. If the support satisfies national interests and policy objectives, it is part of the strategic level CI support. When the

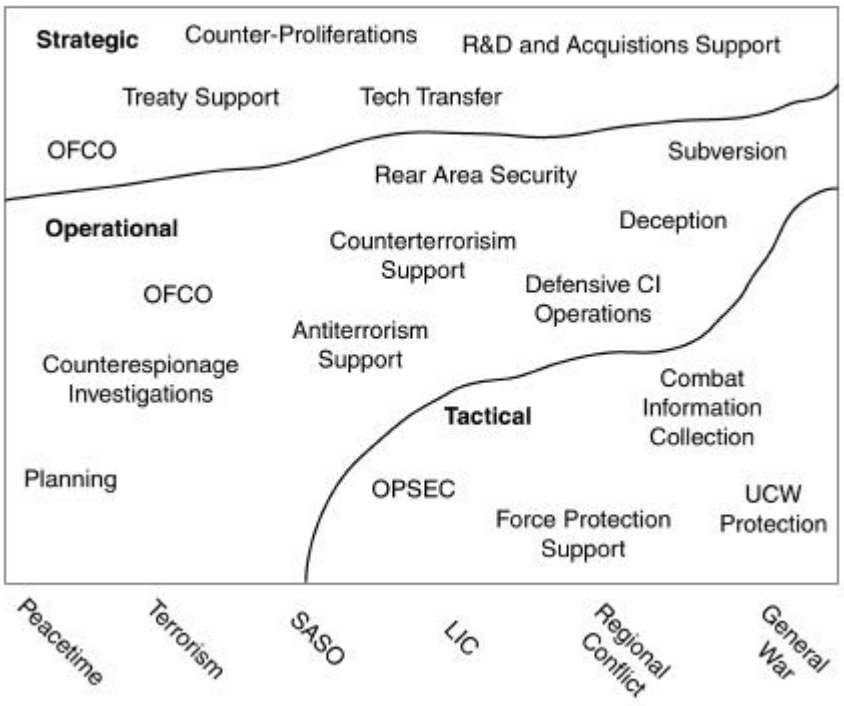

Figure 2-1. Levels of Counterintelligence Support.

objectives and requirements focus on the overall joint force and its operations and sustainment, CI support is at the operational level. Tactical CI support addresses the immediate needs of commanders, particularly maneuver commanders, conducting the battles and engagements, with CI support emphasizing force protection from proximate threats. This publication will focus predominantly on tactical CI support to MAGTF operations.

Strategic CI Support

The strategic level focuses on security objectives, and involves the National Command Authorities, National Security Council, JCS, and Congress. This is a macro perspective in looking at how the instrument of national power is used to satisfy the overarching national objectives, interests, and policies.

Marines support these programs independently and are fully integrated into these programs conducting CI operations, often under the sponsorship of another service or national agencies.

Strategic-level CI helps provide answers to the question, "What threats exist to the national interests and instruments of national power?" Strategic CI primarily supports national-level programs and satisfies requirements across the spectrum of potential threats. Strategic CI emphasizes systems protection, acquisition, proliferation, and strategic level offensive CI operations (OFCO). Although the above programs may also impact on the operational and tactical level, they are generally focused on addressing national-level requirements and support. The impact of these programs should be on national-level decisionmaking with direct linkages supporting combatant commands' strategies and initiatives. National-level agencies centrally manage and control strategic CI support, since the scope of these operations spans across geographic regions and Service or organizational lines.

Operational CI Support

The operational-level commander is the principal supported commander at this level; MAGTF commanders also are key recipients of operational level CI support.

The operational level looks at how to translate the national strategy and objectives into reality through the use of assigned forces. Although strategy—derived from national policies and objectives—defines the nature of the operations, the operational level is responsible for the specific implementation of those strategies. The operational level links strategic security objectives to the tactical decisionmaking and the employment of forces. It is the level that wars are conducted. The operational level looks at the design, organization and integration of strategies, campaigns, and major operations.

Operational CI support, across the joint spectrum of potential employment, is probably the most active area of CI support. It has a major impact on the overall ability of commanders to conduct operations in support of national objectives. Operational CI focuses more on threats to plans and operations, particularly within the context of the wider scope of the campaign, than the more specific scope of the tactical commander. Operational CI focuses on the question of "What are the threats to continuity and the ability to retain the tempo of overall operations?" Operational level CI emphasizes contingency planning, liaison, collections (including CFSO), counterespionage investigations, offensive and defensive CI operations, analysis, production and dissemination of threat related reporting. In contingencies and warfare, many operational CI activities focus on the rear areas, since that is where critical C2, logistics and other sustainment are located.

The combatant command's joint intelligence center and the JTF joint intelligence support element are the principal planners and producers of operational CI support.

Tactical CI Support

Tactical CI is tailored to the needs of the MAGTF and subordinate commanders and addresses their immediate and continuing need for intelligence relating to all manner of threats posed against their forces.

The integration, sustainment, and protection of tactical level forces are of primary concern at this level. The perspective focuses on supporting strategic and operational objectives by implementing and achieving tactical objectives through the use of tactical forces. To a great extent, the tactical level looks at the application of resources (means) applied to achieve national objectives (ends). Responsibility for fighting battles and engagements rests with tactical commanders. Tactical CI support emphasizes direct support to tactical commanders' intelligence and force protection requirements and operations through the identification, neutralization/destruction, and potential exploitation of threats to maneuver forces through the collection of threat related information.

CI personnel conduct vulnerability assessments to look within the command's overall security posture and provide threat assessments to evaluate the infrastructure, capabilities, and intentions of potential threats to the command. They also provide commanders with assessments of the civil population within the AO, and determine their response to the MAGTF presence and actions. The following provides typical examples of CI tactical support.

Non-combatant Evacuation Operations

CI elements deploy to the embassy and other evacuation sites to coordinate and validate the screening of evacuees and assist at the evacuation site to ensure no one attempts to infiltrate with the evacuees.

Peace Operations

CI helps identify and monitor the warring factions and possible third parties to determine potential threats to the peacekeeping/peace enforcement forces.

Humanitarian and Disaster Relief

CI helps identify potential threats to the relief force, providers of aid and assistance, and aid recipients. Often the situation requiring assistance is caused by conflict and can flash with little warning.

Psychological Operations

Psychological operations are normally an activity embedded within other operational activities. CI can assist in gauging the effectiveness of psychological operations and special contingency planning.

Due to the intelligence requirements of commanders in direct contact with hostile forces, the line between CI and HUMINT at the tactical level is blurred almost beyond differentiation. Ground order of battle intelligence is a key area of CI HUMINT collections and production support and seeks to identify enemy forces, dispositions, capabilities, and vulnerabilities. In particular, the identification of threats posed against the MAGTF and the development of countermeasures are key areas CI supports. Intel bn's CI and HUMINT elements are typically task organized into HUMINT support teams (HST). HSTs can satisfy both CI and HUMINT requirements through the collection of threat information from all sources. The teams accomplish this through collection activities including CFSO, overt tactical source HUMINT operations, liaison, interrogation, observation, and debriefings. Threat information in a contingency environment is highly perishable and may have limited utility to anyone other than forces in direct contact.

The standard reporting vehicles are the CI Information Report and the CI SALUTE Report. In addition to this time-sensitive direct support, the intelligence operation center's (IOC) P&A cell is the other key MAGTF producer of tactical CI and HUMINT support.

2004. GARRISON SUPPORT

The primary peacetime/garrison mission of MAGTF CI activities is planning, preparing, and training to accomplish tactical CI functions. A secondary mission is to advise and assist commanders in the planning, coordinating, and implementing of command security and force protection efforts. See chapter 10 for additional information on garrison CI services.

CHAPTER 3. ORGANIZATION AND RESPONSIBILITIES

3001. GENERAL

CI, like intelligence, supports all warfighting functions across the spectrum of military operations. Its effective integration within the intelligence effort requires a basic understanding of the national through tactical intelligence organizations. Commanders, through their intelligence officers, depend on coordination and support from many organizations to satisfy their CI and operational requirements.

3002. COMMANDERS AND STAFF PRINCIPALS

Commander

Intelligence and CI are inherent and essential command responsibilities that require the personal involvement of the commander. Commanders at command echelons are responsible for formulating CI plans and implementing CI measures. Commanders must have an understanding of the capabilities and limitations of CI-an understanding of concepts and theory, practical capabilities, limitations and support requirements of their CI personnel, systems, procedures, operations, and products. They must specify CI requirements, focus their efforts and operations, and provide any necessary guidance to ensure timely and useful products and support. CI activities and measures help the commander shape the battlefield for a decisive action. CI measures support effective command security and force protection operations.

While the intelligence officer advises, plans, and implements command CI activities, the commander ultimately determines the effectiveness of the CI effort.

Intelligence Officer

The intelligence officer (G-2/S-2) manages these efforts for the commander, acting as principal advisor on intelligence and CI, and implement activities that carry out the commander's responsibilities. The commander relies on the intelligence officer to provide the necessary information and intelligence on the weather, terrain, and enemy capabilities, status, and intentions. The intelligence officer is a full participant in the commander's decisionmaking process, ensuring that intelligence and CI are effectively used throughout the command during all phases of mission planning and execution.

Through the intelligence operations plan and supporting intelligence, CI and reconnaissance and surveillance plans, the G-2/S-2 validates and plans IRs, coordinates intelligence priorities, integrates collection, production and dissemination activities, allocates resources, assigns specific intelligence and reconnaissance missions to subordinate elements, and supervises the CI and overall intelligence and reconnaissance efforts.

The commander directs the intelligence and CI effort. The intelligence officer has staff responsibility for intelligence and intelligence operations, including CI.

The G-2/S-2's CI responsibilities parallel basic intelligence responsibilities and include—

- Facilitate understanding and use of CI in the planning and execution of operations.
- Use CI to support situation development and the commander's estimate of the situation through the identification of enemy capabilities, strengths, and vulnerabilities as well as opportunities and limitations presented by the environment.
- Provide necessary CI support to command security and force protection operations.
- Assist the commander in developing priority intelligence requirements and supporting CI requirements.
- Develop and answer outstanding MEF and subordinate units' PIRs and IRs by planning, directing, integrating, and supervising organic CI and multi-discipline MEF and supporting intelligence operations.
- Prepare appropriate CI and other intelligence and reconnaissance plans and orders for the MEF and review and coordinate the CI and all-source intelligence plans of JTFs, theaters, and other organizations.
- Supervise the integration of CI in the development and dissemination of all-source intelligence products tailored to the unit's mission and concept of operations.
- Submit and coordinate all-source and CI collection, production, and dissemination requirements beyond the capability of the MEF to satisfy to higher headquarters for JTF, theater, or national CI systems support.
- Evaluate JTF, theater, and national CI and all-source intelligence support and adjusting stated IRs, if necessary.
- Ensure that the command's intelligence and CI requirements are received, understood, and acted on by organic and supporting intelligence assets as part of an integrated, all-source intelligence effort.
- Ensure that CI and other intelligence information is rapidly processed, analyzed, and incorporated where appropriate in all-source intelligence products, and rapidly disseminated to MEF and external units requiring these.
- Monitor the effectiveness of CI activities and the flow of CI products throughout the command and initiate timely corrective action as appropriate.
- Identify and correct deficiencies in CI and other intelligence and reconnaissance personnel and equipment resources.
- Incorporate exercise CI in training exercises to improve MEF individual, collective, and unit readiness.

Operations Officer

The operations officer (G-3/S-3) is the commander's principal staff assistant in matters pertaining to organization, training and tactical operations. In addition to planning, coordinating and supervising the tactical employment of units, the G-3/S-3's principal responsibilities requiring CI support include—

- Planning and coordinating command security (to include operations and signals security).
- Planning and coordinating command force protection operations.

- Recommending missions and, with the intelligence officer, coordinating reconnaissance and counterreconnaissance operations.
- Planning and coordinating electronic warfare and command and control warfare operations and activities (to include electronic protection and C2 protection).

3003. MEG G-2 SECTION AND INTELLIGENCE BATTALION

G-2 Operations Officer

The G-2 operations officer, under the direction of the MEF AC/S G-2, has primary responsibility for intelligence support to the CG and the remainder of the MEF CE in support of current operations and future operations. Specific all-source intelligence and key CI related duties include (see figure 3-1)—

- Coordinating and providing intelligence and CI support to the CG, the G-3 operations section, and the rest of the MEF CE's battlestaff.
- Serving as the G-2 representative to the MEF CE crisis action team.
- Coordinating, providing and supervising intelligence and CI support to the MEF CE current operations center (COC), future operations center (FOC), and force fires.
- Planning, directing, and supervising the Red Cell.

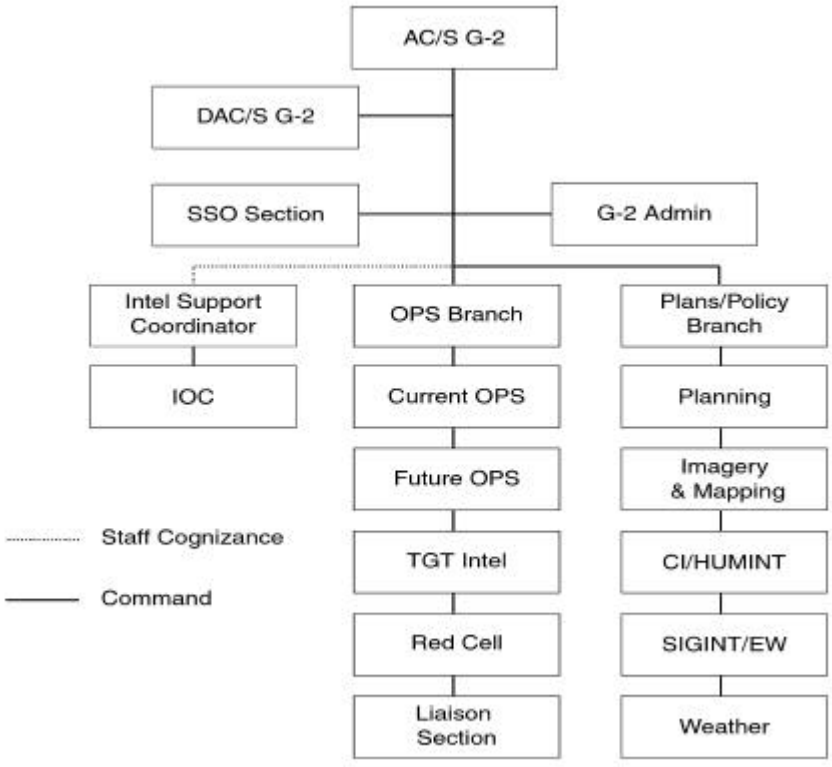

Figure 3-1. MEF G-2 Division Principal Staff Officers and Relationships.

- Providing recommendations on PIR and IR validation, prioritization, and tasking to the AC/S G-2 and the ISC.
- Coordinating and supervising the transition of intelligence and CI planning and operations from G-2 plans to G-2 future operations, and from G-2 future operations to G-2 current operations, to effectively support the MEF's single battle transition process.
- Planning, directing, and supervising MEF liaison teams to external commands (e.g., the JTF and joint functional components headquarters) and intelligence organizations.
- Coordinating with the ISC and MEF MSCs' G-2 operations officers to ensure unity of effort of MEF intelligence and CI operations.
- Providing intelligence and CI input and other support to MEF warning and fragmentary orders and to operations related reporting (e.g., periodic situation reports).
- Coordinating intelligence and CI training for the MEF G-2 section and providing G-2 oversight for and integration of the entire MEF intelligence training program.
- Other intelligence and CI support and tasks as directed by the AC/S G-2.

G-2 Plans Officer

The G-2 plans officer, under the direction of the MEF AC/S G-2, has primary responsibility for intelligence support to the MEF CE's future plans cell. Specific all-source and key CI related duties include (see figure 3-1)—

- Planning the MEF concept of intelligence operations for approval by the AC/S G-2 and subsequent implementation by the ISC based upon the mission, threat, commander's intent, guidance, and concept of operations. This concept of intelligence operations will include a supporting CI concept of operations.
- Leading, coordinating and providing intelligence and CI support to MEF G-5 future plans section.
- Planning and coordinating intelligence and CI support requirements for and the deployment of intelligence elements and resources into the AO.
- Providing recommendations on PIR and IR validation, prioritization, and tasking to the AC/S G-2 and the ISC.
- Coordinating, with the ISC, G-2 development of Annex B (Intelligence) to MEF operations plans (OPLAN), their supporting appendices (such as the initial appendix 3, Counterintelligence, and appendix 5, Human Resources Intelligence), and all intelligence input to other annexes of OPLANs.
- Keeping the G-2 section, other CE staff sections, intelligence liaison personnel, augmentees, and others as appropriate apprised of MEF intelligence and CI planning actions and requirements.
- Identifying requirements and providing recommendations to the G-2 operations officer for MEF intelligence liaison teams to external commands (e.g., the JTF or other components' headquarters) and intelligence agencies.
- Coordinating and developing policies for MEF intelligence, CI and reconnaissance operations.

- Planning, directing, and supervising the MEF G-2's imagery and mapping, CI/HUMINT, SIGINT, and weather sections.
- Accomplishing other intelligence and CI support and tasks as directed by the AC/S G-2.

Intel Bn Commander/Intelligence Support Coordinator

The intel bn commander is responsible for planning and directing, collecting, processing, producing and disseminating intelligence, and providing CI support to the Marine expeditionary force (MEF), MEF MSCs, subordinate MAGTFs, and other commands as directed.

Garrison Operations

In garrison the principal task of the intel bn commander is to organize, train, and equip detachments that support MAGTFs or other designated commands to execute integrated collection, intelligence analysis, production, and dissemination of intelligence products. The composition of intel bn is shown in figure 3-2.

Actual Operations

During operations, the intel bn commander is dual-hatted as the ISC, serving as such under the direct staff cognizance of the MEF AC/S G-2 (see figure 3-1). During garrison operations, many of the tasks listed here are the responsibility of the G-2 operations officer. The intel bn's S-3 section along with the operations center element of the MEF G-2 form the core of the ISC support effort, with planning, direction, and C2 conducted within the IOC's support cell. The ISC is responsible to the MEF AC/S G-2 for the overall planning and execution of MEF all-source intelligence operations. Specific

During garrison operations, many of the tasks listed here are the responsibility of the G-2 operations officer.

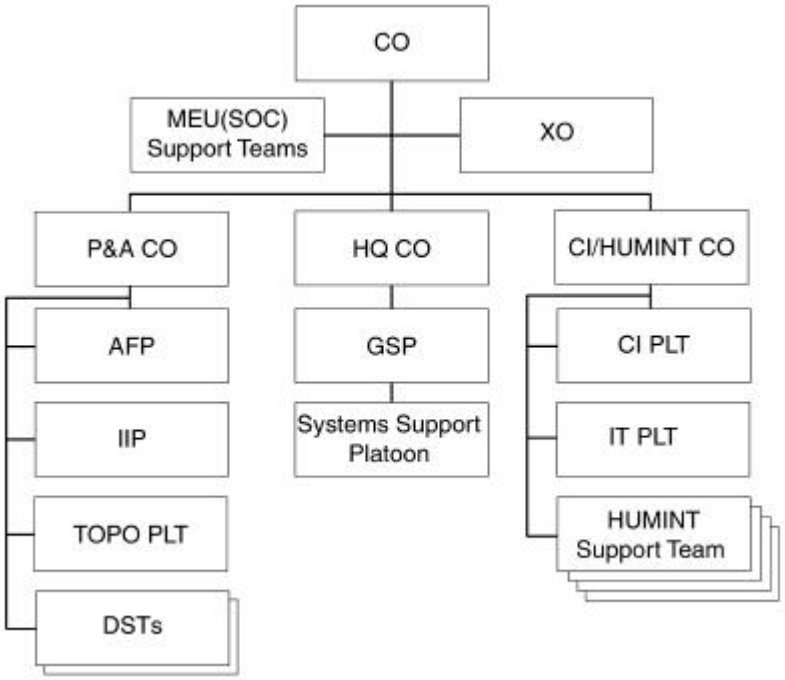

Figure 3-2. Intelligence Battalion.

all-source and key CI responsibilities of the ISC during actual operations include—

- Implementing the concept of intelligence operations and the supporting CI concept of operations developed by the G-2 plans officer and approved by the AC/S G-2.
- Establishing and supervising operation of the MEF intelligence operations center (IOC), including the support cell, the surveillance and reconnaissance cell (SARC), and the P&A cell (see figure 3-3.) Generally the IOC will be co-located with the MEF CE's main command post.
- Establishing and supervising operation of the intel bn's CI/HUMINT company command post.
- Developing, consolidating, validating, and prioritizing recommended PIRs and IRs to support MAGTF planning and operations.
- Planning, developing, integrating, and coordinating MEF intelligence and CI collection, production, and dissemination plans, including the effective organic and external integration and employment of MAGTF CI as well as staff cognizance of MEF SIGINT, IMINT, HUMINT, geographic intelligence (GEOINT), ground remote sensors, ground reconnaissance, and tactical air reconnaissance intelligence collections, production, and dissemination operations.
- Developing, with the G-2 plans officer and G-2 operations officer, and completing Annex B, Intelligence to MEF operations orders (OPORD), supporting appendices (such as appendix 3, CI), and intelligence and CI input to other annexes of OPORDs.
- Planning, developing, integrating, and coordinating intelligence and CI support to the commander's estimate, situation development, indications and warning, force protection, targeting, and combat assessment.
- Managing and fusing the threat (or red) COP/CTP inputs from subordinate units and external commands and intelligence agencies into the MEF CE's threat COP/CTP.
- Providing intelligence and CI support to the MEF CE G-2 section and the MSCs.
- Preparing the intelligence and CI estimates to support G-2 plans.

The ISC is tasked to perform PIR and IR validation and prioritization only during actual operations when the IOC is activated. During routine peacetime operations the PIR/IR validation and prioritization task is the responsibility of the MEF CE's G-2 operations officer.

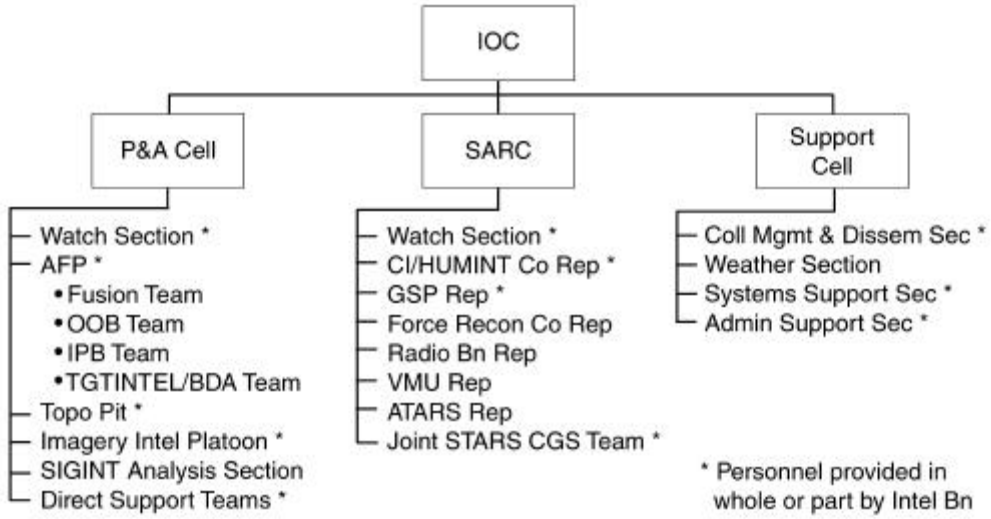

Figure 3-3. Intelligence Operations Center.

- Planning, developing, and coordinating intelligence communications and information systems architecture, including its integration and support of MEF CI and other intelligence and reconnaissance requirements.
- Coordinating and integrating MEF CI and all-source intelligence operations with other service components, JTF joint intelligence support element (JISE) and the joint force J-2 CI/HUMINT staff element (J-2X), theater joint intelligence center (JIC) or joint analysis center (JAC), and national intelligence agencies and operations (e.g., NIMA), including all aspects of intelligence and CI reach-back support.
- Assisting with the evaluation and improvement of MEF CI and all-source intelligence operations.
- Accomplishing other intelligence and CI support and tasks as directed by the AC/S G-2.

(See table 3-1 for a summary of the principal responsibilities of the AC/S G-2's three principal staff subordinate officers.)

CI/HUMINT Officer

During garrison operations the CI/HUMINT Officer (CIHO) is responsible to the G-2 plans officer, in coordination with the intel bn commander, for the planning, direction, and execution of MEF CI/HUMINT operations. In intelligence sections without a CIHO, a designated officer will generally be assigned to perform these tasks. If a HST or other CI/HUMINT Co element is attached, its senior CI/HUMINT officer will serve in this capacity. During action operations, the CIHO's specific duties include—

- Preparing MAGTF CI/HUMINT concept of operations, plans and orders; and directing, coordinating and managing organic and supporting CI/HUMINT operations with the intel bn commander/ISC, G-2 plans officer, IOC's support cell OIC, and the CI/HUMINT company commander.
- Coordinating, planning, supervising, and assisting CI collection requirements and taskings for MAGTF operations with the intel bn commander/ISC, collection management and dissemination officer (CMDO) and CI/HUMINT Co planners.
- Maintaining liaison with other CI and HUMINT agencies.

Table 3-1. AC/S G-2's Principal Subordinate Staff Officers and Their Responsibilities.

ISC	G-2 Ops O	G-2 Plans O
Planning and execution of intel ops to support all MEF IRs	Intelligence support to MEF CE battle-staff and current ops center agencies	Intelligence support to the G-5 future planning team for future planning IRs.
Establish and direct the IOC (P&A Cell, SARC, and Support Cell)	Coordinate and support to higher and adjacent HQs and agencies	Recommends IR validation, prioritization and tasking to AC/S G-2
IR management (collection, production, and dissemination) validation, prioritization, and tasking per AC/S G-2 direction	Recommends IR validation, prioritization, and tasking to AC/S G-2	Establish and direct the G-2 future planning intelligence element
Intel ops command of Intel bn and staff cognizance over SIGINT, CI, HUMINT, MASINT, IMINT, and air-ground recon (includes staff cognizance of designated G-2 elements)	Establish and direct intelligence elements and support to the COC, FOC, Tgt Intel Sec, force fires, Red Cell, and MEF intelligence liaison teams	G-2 section's imagery and mapping, CI/HUMINT, SIGINT, and weather sections (less that under staff cognizance of the ISC)

In intelligence sections without a CIHO, a designated officer will generally be assigned to perform these tasks. If an HST or other CI/HUMINT Co element is attached, its senior CI/HUMINT officer will serve in this capacity.

- Planning for the timely reporting of CI/HUMINT-derived intelligence to MAGTF and external elements and the rapid handling of perishable CI/HUMINT information with the intel bn commander/ISC and CMDO.
- Assisting the intel bn commander/ISC, G-2 plans officer, and G-2 operations officer with preparing and presenting intelligence briefings and reports as required.
- Serving as the principal point of contact between the command and NCIS in matters involving the investigation of actual, potential, or suspected espionage, sabotage, terrorism intelligence, and subversive activities, including defection, ensuring that information about these activities is reported promptly to the nearest NCIS representative. Informing the Criminal Investigation Division (CID) of the Provost Marshal Office (PMO) on criminal matters. These include those of a terrorist nature uncovered in the course of a CI investigation.
- Monitoring command CI/HUMINT MOS training and providing advice and assistance for the maintenance of an effective program.
- Coordinating with the G-2 operations officer, ISC and G-3 to provide CI support to the command's force protection mission, including OPSEC, and deception.
- Providing personnel to jointly man the CAT with CID, NCIS, and if required, civilian law enforcement agents when a crisis action team is established in response to a terrorist or criminal situation,.
- Assuming the role as the Task Force CI Coordinating Authority (TFCICA) when the MAGTF CE is designated as a JTF headquarters.

Collection Management/Dissemination Officer

The CMDO is sourced from the intel bn's S-3 section and is a key subordinate to the intel bn commander/ISC during operations. The CMDO is responsible for formulating detailed intelligence and CI collection requirements (ICRs) and intelligence dissemination requirements (IDR) and tasking and coordinating internal and external operations to satisfy these. The CMDO receives validated PIRs and IRs and direction from the ISC, and then plans and manages the best methods to employ organic and supporting collection and dissemination resources through the intelligence collection and dissemination plans (tabs to Appendix 16, Intelligence Operations Plan, to Annex B), which includes CI collection and dissemination activities. The CMDO is responsible for validating and forwarding national and theater CI and other collection requests from the MEF and MSCs typically using appropriate intelligence and CI tools and TTP. The CMDO is also responsible for coordinating intelligence and CI CIS requirements and maintaining awareness of available CIS connectivity throughout the MAGTF and with key external organizations. During operations the CMDO works within the support cell (see figure 3-3). With the P&A cell OIC, the SARC OIC, G-2 operations officer, CI/HUMINT Co CO, and the MEF G-6, the CMDO is responsible to the ISC for the following CI-related tasks:

- Determining and coordinating the collection effort of PIRs/IRs via organic and supporting CI resources.
- Evaluating the effectiveness of MEF and supporting CI collection and dissemination operations.

- Determining PIRs/IRs and preparing requests for intelligence (RFI) that are beyond organic capabilities and preparing submissions to higher headquarters and external agencies for support.
- Recommending dissemination priorities, development of intelligence and CI reporting criteria, and advising and selecting dissemination means.
- Developing and coordinating CI and all-source intelligence collection plans, coordinating and integrating these with MEF, other components, JTF, theater, and national intelligence collection and dissemination operations.
- Developing and coordinating CI and all-source intelligence dissemination plans and supporting architectures for both voice and data networked communications, and coordinating and integrating these with MEF, other components, JTF, theater, and national intelligence CIS and dissemination operations.
- Monitoring the flow of CI throughout the MAGTF and ensuring that support is delivered to intended recipients in a timely fashion and satisfactorily meets their needs.

Surveillance and Reconnaissance Cell OIC

The SARC OIC is also an immediate subordinate of the ISC and is responsible for supervising the execution of the integrated organic, attached, and direct support intelligence collection and reconnaissance operations (see figure 3-3). The SARC OIC is responsible to the ISC for accomplishing the following specific CI-related responsibilities:

- Coordinating, monitoring, and maintaining the status of all ongoing CI collection operations. This includes—
  - Missions, tasked ICRs, and reporting criteria for collection missions.
  - Locations and times for pertinent fire support control measures.
  - Primary and alternate CIS plans for both routine and time-sensitive requirements, for CI collectors as well as collectors or the SARC and key MEF CE and MSC C2 nodes, to support ongoing C2 of CI collection operations and dissemination of acquired data and intelligence to those needing it via the most expeditious means.
- Conducting detailed CI collection planning and coordination with the MSCs and CI/HUMINT Co planners, with emphasis on ensuring understanding of the collection plan and specified intelligence reporting criteria.
- Ensuring other MAGTF C2 nodes (e.g., the current operations center, force fires, etc.) are apprised of ongoing CI and other intelligence and reconnaissance operations.
- Receiving routine and time-sensitive CI-related reports from deployed collection elements; cross-cueing among intelligence collectors, as appropriate; and the rapid dissemination of CI reports to MAGTF C2 nodes and others per standing PIRs/IRs, intelligence reporting criteria, the dissemination plan, and the current tactical situation.

Production and Analysis Cell OIC

The P&A cell OIC is the third principal subordinate to the ISC, with primary responsibility for managing and supervising the MEF's all-source intelligence and CI processing and production efforts (see figure 3-3 on

page 3-6), including aspects of CI production. Key all-source and CI-related responsibilities include—

- Planning, directing, and managing operations of the all-source fusion platoon (to include the fusion, order of battle, IPB, and target intelligence/ battle damage assessment teams), the topographic platoon, the imagery intelligence platoon (IIP), the direct support teams (DST), and other analysis and production elements as directed.
- Coordinating and integrating P&A cell operations, estimates and products with the MEF G-2 section's operations branch and its Red Cell operations and estimates.
- Maintaining all-source-automated intelligence and CI data bases, files, workbooks, country studies and other intelligence studies.
- Planning and maintaining CI, imagery, mapping and topographic resources and other intelligence references.
- Administering, integrating, operating, and maintaining intelligence processing and production systems, both unclassified general service and SCI information systems (e.g., CHATS).
- Analyzing and fusing CI with other intelligence and CI into tailored all-source intelligence products to satisfy all supported commanders' stated or anticipated PIRs and IRs.
- Developing and maintaining current and future intelligence situational, threat, and environmental assessments and target intelligence based upon all-source analysis, interpretation, and integration.
- Managing and fusing the threat (or red) COP/CTP inputs from subordinate units and external commands and intelligence agencies into the MEF CE's threat COP/CTP.

CI/HUMINT Companies

The counterintelligence/HUMINT company (CI/HUMINT Co) is organic to the intel bn within each MEF. CI/HUMINT Co is organized and equipped under tables of organization number 4713 and 4714. It is under the command of the intel bn commander, with any detachments from it under the command of its OIC. The MEF commander exercises command and control of MEF CI/HUMINT operations through the MEF AC/S, G-2, to accomplish the CI/HUMINT mission. The AC/S, G-2 exercises direction of intelligence battalion and the CI/HUMINT company through the intelligence operations officer and the CIHO. The intel bn commander, MEF headquarters group, exercises command and control of the CI/HUMINT Co.

Mission

The mission of the CI/HUMINT Co is to provide CI and HUMINT support to the MEF, other MAGTFs, and other units as directed.

Tasks

- Conduct tactical CI activities and operations, to include CFSO.
- Conduct screening, debriefing, and interrogation of personnel of intelligence/CI interest.
- Direct and supervise intelligence activities conducted within the interrogation facility and the document and material exploitation facility.

- Perform CI and terrorism threat analysis and assist in the preparation of CI and intelligence studies, orders, estimates, and plans.
- Conduct overt HUMINT operations.
- Collect and maintain information designed to identify, locate, and recover captured or missing personnel.
- Debrief friendly personnel recovered from enemy prisoner of war (EPW), hostage or detainee status.
- Translate and exploit captured documents.
- Assist in the conduct of tactical exploitation of captured material and equipment.
- Conduct limited CI investigations during combat or operations other than war.
- Conduct CI surveys and evaluations.
- Conduct TSCM operations.
- Maintain foreign area specialists who provide sociological, economic, cultural and geo-political information about designated countries.

Organization

A CI/HUMINT Co consists of a headquarters section, a CI platoon, an interrogator-translator (IT) platoon and two to five HUMINT Support Teams (HSTs). The CI platoon is organized into a platoon headquarters, four CI teams (CIT), and a TSCM team. The IT platoon is organized into a platoon headquarters and six IT teams (ITT). Figure 3-4 shows the organization of CI/HUMINT Co within I and II MEF (T/O # 4714); figure 3-5 on page 3-12 shows the organization of III MEF's CI/HUMINT Co (T/O # 4713).

Command and Control and Concept of Employment

Command and Control. The CI/HUMINT Co is a subordinate unit of the intel bn, with the intel bn commander maintaining full command of its

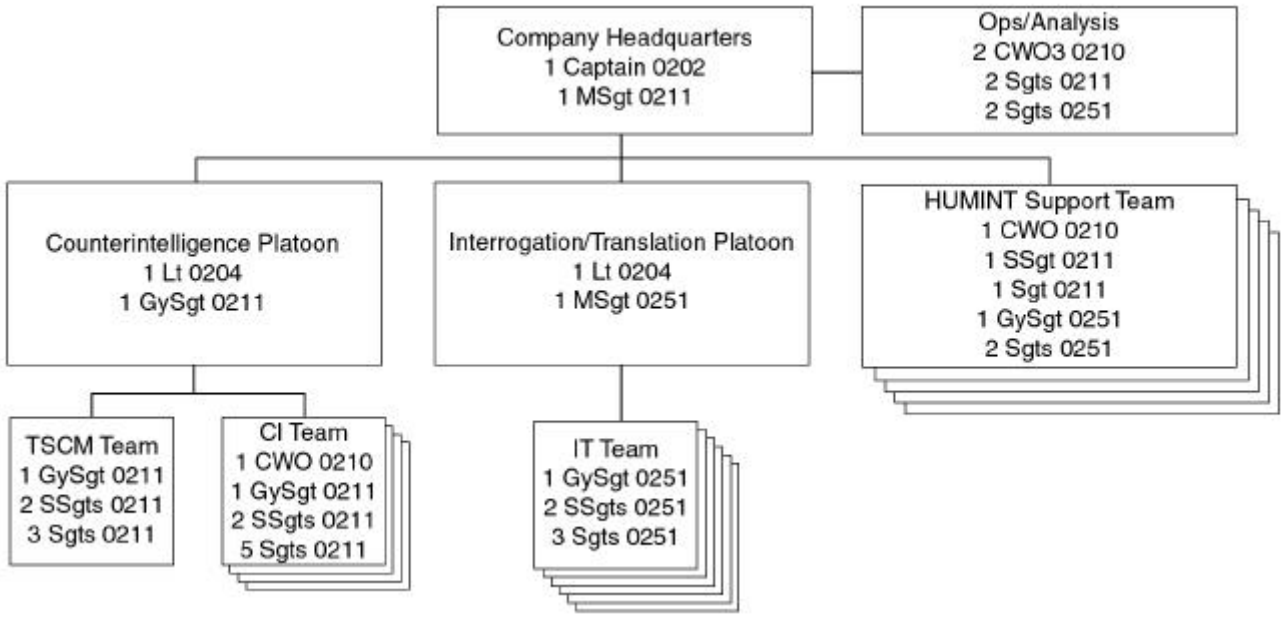

Figure 3-4. CI/HUMINT Company, 1st and 2d Intel Bns, I and II MEF.

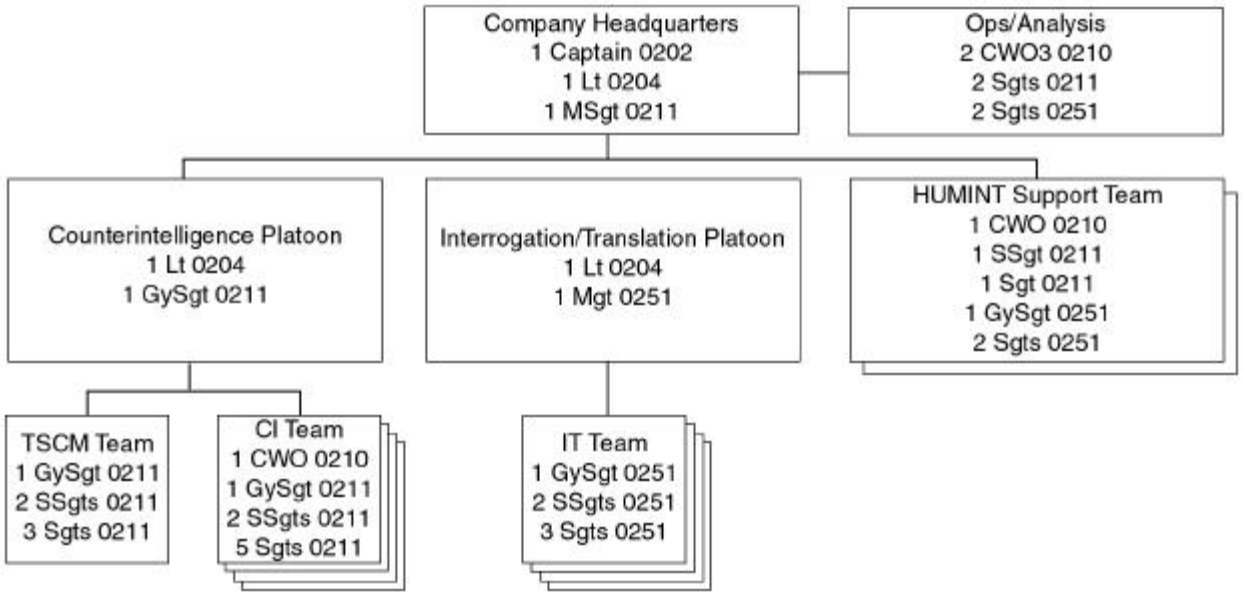

Figure 3-5. CI/HUMINT Company, 3d Intel Bn, III MEF.

operations. The CI/HUMINT Co commander exercises full command authority over subordinate elements, fewer elements that have been detached under a particular task organization. When supporting smaller MAGTFs, CI/HUMINT Co or its detachments will operate under the C2 of either the intel detachment OIC or the supported unit's G-2/S-2. The CI/HUMINT Co is under the command of the intelligence battalion commander. Operational control (OPCON) of intel bn rests with the MEF commander. The MEF commander exercises OPCON through the G-2. Tactical control (TACON) or specified C2 support relationships of CI/HUMINT elements may be provided to MEF subordinate commanders depending upon the situation. However, regardless of the C2 and support relationships, the MEF commander will generally retain technical control of all MEF CI/HUMINT CO elements.

MEF CE Staff Cognizance. The MEF commander will usually exercise C2 over the intel bn elements, to include the CI/HUMINT Co, via the MEF AC/S G-2. The ISC performs this function under the staff cognizance of the AC/S G-2. The intel bn commander/ISC exercises C2 of CI/HUMINT Co via its commanding officer. This allows for the centralized direction and effective integration of CI/HUMINT Co operations within the MEF's broader all-source intelligence concept of operations.

Concept of Employment and C2 Support Relationships. The CI/HUMINT Co combines the MEF's CI and IT capabilities into one organization to provide unity of effort of CI and HUMINT operations in support of MAGTF intelligence and force protection needs. The company is employed per the concept of intelligence support, the CI and HUMINT plans, and the intelligence operations plan developed by the MAGTF G-2/S-2. Subordinate elements of the company may be placed in GS of the MEF, placed in direct support of subordinate commands, or attached to subordinate elements. Additionally, a task-organized detachment will

usually be provided to most subordinate MAGTFs and may be used to support joint operations. Figure 3-6 portrays typical notional concept of employment and task organization of CI/HUMINT Co and its elements.

- **General Support.** CI/HUMINT Co will typically operate in GS of the MEF. Under GS, the MEF commander, through the G-2 and the intel bn commander/ISC, determines priorities of intelligence collections and production support, locations of CI support nodes, and CI and all-source intelligence dissemination.
- **Direct Support and Attached.** Depending upon mission, enemy, terrain and weather, troops and support available, time available (METT-T) factors and considerations, the CI/HUMINT Co or task-organized HSTs or other detachments from it may be employed in direct support of or attached to a particular unit or MSC of the MEF. In such cases the scope of the supported commander's C2 authority over assigned CI/HUMINT Co elements will usually be specified to ensure effective support to his operations while allowing the MEF commander to maintain effective C2 of broader intelligence and CI operations.
- **Technical Control.** TECHCON is the performance of specialized or professional service, or the exercise of professional guidance or direction through the establishment of policies and procedures. The nature of the threat CI targets is such that within the MEF, CI TECHCON generally will be retained, coordinated and exercised by the MEF commander via the AC/S G-2 and exercised via the ISC regardless of any other C2 relationships established for the operation. For example, the MEF commander will generally retain CI TECHCON over CI/HUMINT Co elements attached to or placed in direct support of MAGTF subordinate elements.
- **Annex B and the Intelligence Operations Plan.** Specific details regarding C2 relationships over MAGTF CI/HUMINT company

Staff cognizance—The broad responsibility and authority over designated staff functions assigned to a general or executive staff officer (or their subordinate staff officers) in his area of primary interest. These responsibility and authorities can range from coordination within the staff to the assignment or delegation to the staff officer by the commander to exercise his authority for a specified warfighting function or sub-function. Staff cognizance includes the responsibility for effective use of available resources and may include the authority for planning the employment of, organizing, assigning tasks, coordinating, and controlling forces for the accomplishment of assigned missions. Marine Corps orders and doctrine provide the notional staff cognizance for general or executive staff officers, which may be modified by the commander to meet his requirements. (MCWP 6-2, *MAGTF C2*)

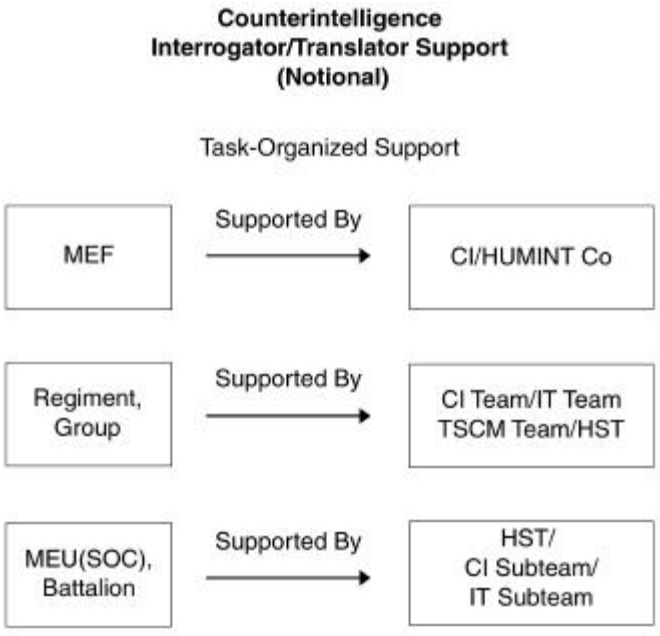

Figure 3-6. CI/HUMINT Company Notional Concept of Employment and Task Organization.

operations and resources will generally be detailed within the operations plan (OPLAN) or OPORD. This usually will be in one of the following documents: Paragraph 5 to the basic annex B; appendix 3 (CI) to annex B; or appendix 16 (Intelligence Operations Plan) to annex B.

Administrative, Logistics, and Other Support

Administrative. CI/HUMINT Co and its subordinate units are not capable of self-administration. Administrative support is provided by the MEF Headquarters Group (MHG). Administrative support for HSTs and CI/HUMINT Co detachments is provided by the supported unit.

Maintenance and Supply. CI/HUMINT Co and its subordinate units are capable of first echelon maintenance support of organic equipment. Higher maintenance is provided by the MHG or other designated external or supported units.

Transportation. CI/HUMINT has limited organic vehicular transportation support to support Co and subordinate units operations. External transportation support from the MHG, other designated unit or the supported unit is necessary to displace all company elements.

Selected Items of Equipment

TAMCN	Description	Nomenclature	Qty
A03809	Counterintelligence Equipment, Tech Surveillance		1
A0890	Facsimile, Digital, Lightweight	AN/UXC-7	9
A1260	Navigation Set Satellite (PLGR)	AN/PSN-11	25
A2030	Radio Set	AN/PRC-68A	2
A2065	Radio Set	AN/PRC-104B(V)	8
A2070	Radio Set	AN/PRC-119A	23
A2145	Radio Set	AN/VRC-46	5
A2167	Radio Set	AN/VRC-88A	20
D0850	Trailer, Cargo, 3/4-ton, two-wheel	M-101A3	7
D1158	Truck, Utility, Cargo/Troop Carrier 1/4-ton, HMMWV	M-998	35

HUMINT Support Team

The HST is the smallest element to deploy in support of a MAGTF and often serves as the basic building block for CI/HUMINT Co support to subordinate elements of the MAGTF. Specific elements and capabilities provided in the detachment will be based upon the mission of the supported unit, commander's intent, results of the intelligence preparation of the battlespace, the supported unit's concepts of operations and intelligence, and other METT-T factors.

Mission

HSTs support the MAGTF's focus of effort or other designated units, exploit significant HUMINT or CI collection opportunities, or provide tailored support to individual subordinate elements of the MAGTF, in particular

elements operating independently from the rest of the MAGTF. For example, a HST is usually attached to the Marine expeditionary unit (special operations capable) MEU (SOC) command element.

Tasks

- Conduct offensive and defensive CI activities, including counterespionage, countersabotage, countersubversion, and counterterrorism in support of tactical units.
- Conduct intelligence collection operations using CFSOs and overt tactical source HUMINT operations.
- Advise commanders concerning support to their force protection, OPSEC, deception, and security programs.
- Assist in the preparation of CI estimates and plans for AO reflected by concept/operation plans.
- Maintain information and CI data bases concerning personalities, organizations, installations, and incidents of CI interest in support of concept/operation plans.
- Collect and maintain information designed to identify, locate, and recover friendly personnel captured, mission (non-hostile), and missing in action.
- Conduct CI debriefings of friendly EPWs who are returned to U.S. control.
- Conduct liaison with unit, JTF, other services, allied, and host nation intelligence and local intelligence, CI, and law enforcement agencies as appropriate.
- Conduct CI investigations about espionage, sabotage, terrorism, subversion, and defection; and other special CI investigations, during combat operations per theater directives.
- Conduct debriefings/interrogation of known or suspected foreign intelligence personnel and agents taken prisoner.
- Maintain foreign language proficiency to support operations.
- Assist in Cl surveys/vulnerability assessments of commands and installations to determine the security measures necessary to protect against espionage, sabotage, subversion, terrorism, and unauthorized disclosure or access to classified material.
- Debrief Marine Corps personnel detained/held hostage by foreign governments or terrorist organizations.

T/Es for CI/HUMINT company had not been finalized by the time of publication of this manual. Refer to the current tables of equipment for accurate current information.

Organization

HSTs combine CI and IT personnel in a single unit to integrate CI and HUMINT collection capabilities. The HST normally consists of one CI officer, two CI enlisted specialists, and three enlisted ITs. Its specific composition, however, will be based upon the mission. HSTs are capable of planning and executing CI/HUMINT operations supporting the designated unit's intelligence and force protection requirements.

Command and Control and Concept of Employment

Command and Control. HSTs are normally attached to the units they support, but they may be placed in direct support. When attached they are OPCON to the supported commander, who exercises C2 via the unit's intelligence officer. Finally, TECHCON of HST operations generally will be

retained by the MAGTF commander and exercised via the MAGTF G-2/S-2 and the ISC.

Concept of Employment. HSTs will be employed per the supported commander's concepts of intelligence and operations and the specified C2 relationships.

3004. INDIVIDUAL MARINES

Marines—regardless of rank or military occupational speciality (MOS)—will ensure that their unit's security is not compromised through comprehensive understanding of the unique security vulnerabilities of their operations and functions and the enforcement of necessary personnel, information, operations, and electronic security measures.

3005. MARINE CORPS CI ORGANIZATIONS WITHIN THE SUPPORTING ESTABLISHMENT

The Director of Intelligence is responsible to the CMC with primary responsibility for developing and monitoring Marine Corps CI policy implementation throughout the Marine Corps. The Head, CI/HUMINT Branch of the Intelligence Department, Headquarters U.S. Marine Corps is the principal advisor to the Director of Intelligence for CI/HUMINT matters. The CI/HUMINT Branch performs the following functions:

- Prepares plans, policies, and directives, and formulates controlled CI/HUMINT missions.
- Coordinates with national-level Department of Defense (DOD) and non-DOD agencies on matters dealing with Cl and HUMINT.
- Acts as the CI military occupational specialty (MOS) sponsor (MOS 0204/0210/0211) and IT MOS sponsor (MOS 0251).
- Maintains staff cognizance over CI field units and staff management of training.
- Exercises staff responsibility for HUMINT resources and certain classified/special access programs.
- Coordinates with the NCIS in special investigations and operations.
- Conducts security reviews.
- Reviews reports from the field commands concerning security violations, loss of classified material, and compromises.
- Coordinates the release of information for foreign disclosure.
- Represents the Marine Corps on national level interagency CI committees and subcommittees.

3006. NAVAL COMPONENT ORGANIZATION

N-2 Intelligence Officer

While afloat, the N-2 coordinates activities of the attached NCIS agent to identify threats to the amphibious ready group (ARG). The N-2 coordinates vulnerability/threat assessments and other intelligence and CI in support of ARG intelligence and force protection requirements for the ships. Close coordination between the MAGTF G-2/S-2 and the N-2 ensures consolidation and dissemination of applicable threat related data for the formulation of the commander's estimate. Monitoring and rapid reporting of time sensitive information and intelligence is critical for these deployed commanders as the situation develops. The critical role is the monitoring for indications and warning of impending attack during movement or the deployment of forces ashore. The ARG/MAGTF team continues this interactive relationship through the rapid collection, processing, production, and dissemination of intelligence and CI support of intelligence and force protection requirements.

Attached NCIS Agent

With MAGTF CIHO and other CI elements, the NCIS agent afloat assists the command with the identification of threat and vulnerabilities of the ARG. As a special staff officer under the staff cognizance of N-2, the NCIS agent also has the responsibility for criminal investigation with the ship's master-at-arms and the MAGTF CID officer. During contingency operations, the NCIS agent serves as the principal planner and host for NCIS's surge capability via its Special Contingency Group. The Special Contingency Group is a task-organized group of specially trained NCIS agents prepared and equipped for deployment into tactical situations.

3007. JOINT CI ORGANIZATION

In accordance with DODINST 5240.10, *DOD Counterintelligence Support to Unified and Specified Commands*, each combatant command has a special staff officer within the J-2 with staff cognizance for CI activities within the theater.

CI Staff Officer

The CI Staff Officer is the J-2's primary staff officer responsible for advising, planning, and overseeing theater CI activities. Responsibilities include—

- Advise commander and J-2 on CI investigations, operations, collections, and production activities affecting the command.
- Advise commander on counterdrug, OPSEC, counterterrorism, and antiterrorism activities in the command area of responsibility (AOR).
- Coordinate CI support activities within combatant command's headquarters staff and with component organizations.
- Coordinate the combatant commander's CI requirements with pertinent U.S. CI organizations and U.S. country teams as required.
- Coordinate tasking of CI within AOR and area of interest on implementation of NCA approved/directed action.

- Coordinate with the military services for integrated CI support to research and development and acquisition programs to protect sensitive or critical technologies.
- Ensure significant CI threat information developed within commander's AOR is forwarded to the J-2, other staff officers, and subordinate component commanders.
- Ensure CI support requirements are identified and satisfied during development of command intelligence architecture plans.
- Ensure CI staffing and analytic and production support is integrated into the combatant command's JICs.
- Ensure CI collection, production, and dissemination priorities are integrated into command's intelligence operations plans.

Task Force CI Coordinating Authority

The task force CI coordinating authority (TFCICA) is a JTF headquarters staff officer designated by the combatant commander as the executive agent for CI activities within a JTF's AOR. The TFCICA coordinates and deconflicts with the Defense HUMINT Service's representative to the JTF and the HUMINT Operations Cell (HOC). Together these two staff responsibilities combine to create the JTF headquarters J-2X, which has the task of coordinating and deconflicting CI and HUMINT activity within the JTF AOR. This includes coordination with the U.S. country team and any external attachments and agencies conducting CI and HUMINT activity within the AOR.

3008. NATIONAL LEVEL COUNTERINTELLIGENCE SUPPORT

The Defense Intelligence Agency (DIA) is critical in the planning and establishment of military CI activities.

DIA is the principal DOD organization for CI analysis and production in support of DOD requirements. It focuses on hostile threat and foreign intelligence and security services, to include the development, population and maintenance of CI data bases for personalities, organizations, and installations (PO&I). PO&I files become the cornerstone of the CI activities planning and targeting, and guide CI and HUMINT activities. DIA's Defense HUMINT Service (DHS) is the force provider for strategic HUMINT forces and capabilities. During operations, elements from DHS form a partnership within the supported JTF headquarters' J-2X element for the coordination and deconfliction of HUMINT-source related collection activities.

CHAPTER 4. COUNTERINTELLIGENCE EMPLOYMENT

4001. OPERATIONAL ENVIRONMENT

As forces are committed to an operation, the threat picture expands and situational awareness improves. As U.S. military involvement increases, existing threats remain and may increase while new threats may emerge. In humanitarian operations and other MOOTW, the principal threats facing the MAGTF are criminal, terrorist, and espionage. These threats continue into the upper levels of conflict, with the addition of threats posed by irregular forces, special operations forces, and finally, by large-scale conventional military forces.

Within MOOTW and in lesser levels of conflict where there may be no designated MAGTF or joint rear area, CI activities are directed at supporting force protection efforts by engaging with key civic leaders, existing intelligence and security structure, factional leaders and cooperative personnel, and allied forces. Threats are normally at the low to mid level. Threats at higher levels of conflict normally involve conventional or unconventional force threats that require combat forces to counter. MAGTF CI elements conduct actions in support of these operations within the MAGTF area of operations and other assigned sectors as directed (e.g., the joint rear area). Three basic political operational categories can be used to frame CI activities. These are—

The primary operational environmental factor influencing MAGTF CI activities is political, vice physical.

- **Permissive**—An operational environment that specific agreements allow CI to conduct activities independently or with the host nation. In these environments, MAGTF CI activities and support to the security posture of the deployed forces are normally conducted with the host nation, or the host nation has provided concurrence, either direct or tacit.
- **Semi-Permissive**—An operational environment where there are either no in-place government organizations and/or laws, or where the government in power is not duly recognized by the U.S. or other international bodies. In these situations, the rules of engagement established by the JTF or multinational force commander is often the key variable as the host nation's civil, military, and security agencies are frequently degraded or nonexistent (or may even be supporting threat forces). Rules of engagement of the deploying force primarily drive limitations and restrictions that may be placed on CI activities.
- **Non-Permissive**—A non-permissive operational environment is one in which U.S. CI activities and contacts with the host nation are extremely limited, normally at the direction of the host nation. The situation in these countries may also place the U.S. in a situation where the actions of the host nation or individuals in the host nation government may be inimical to those of the U.S. government. In most cases, the host government may severely curtail contacts, normally only through a single point of contact. In some cases, the information provided may be of questionable validity.

MAGTF CI personnel must be aware of the differences in each operational environment and be able to establish operations based on the mission, nature of the environment and threat conditions.

Since much of the threat and vulnerability intelligence will be based on information provided by host nation or other sources, vulnerability assessments must be assessed and rapidly updated as necessary.

CI activities help the MAGTF commander develop estimates of the situation, shape the battlespace, and guide intelligence and force protection operations. The MAGTF commander focuses the CI effort by clearly identifying priority intelligence requirements, careful assignment of CI missions and tasks, and a clear statement of desired results. By orienting CI capabilities, the commander guides who or what are the CI targets and the nature and focus of operations (e.g., whether CI efforts will be designated primarily as defensive CI operations or offensive HUMINT operations).

4002. EMPLOYMENT OF CI ELEMENTS

Command and Control and Concept of Operations

The METT-T factors and the tactical concept of operations govern C2 relationships and the execution of CI plans and operations within the MAGTF. Specific CI concept of operations and C2 relationships will be established in either annex B (intelligence) to the operations order, fragmentary orders or other directives.

General Service

CI elements normally operate in GS of the MAGTF. Operational control of CI elements by the force commander provides the commander with the means to meet the specific operational requirements of the MAGTF and other supported forces with limited organic CI resources.

Direct Support and Attachment

Situational and operational factors may require some CI elements to be either attached or placed in direct support of MAGTF subordinate elements (e.g., during operations involving widely separated units in areas of dense population). In such cases, supported unit commanders employ CI personnel to satisfy their CI requirements or other mission specified by the MAGTF commander.

Technical Control

Regardless of the type C2 relationships established, the MAGTF commander will retain technical control (TECHCON) authority over all MAGTF CI and supporting elements, which will be exercised via the G-2/S-2 and intel bn commander/ISC.

Concept of Employment

MAGTF CI elements can be deployed on an area coverage concept or by unit assignment.

Area Coverage

Geographic AOR. MAGTF CI elements employed under area coverage are assigned a specific geographic AOR. Under area coverage, CI support is provided to commands located within the designated area. CI elements continue to operate within the assigned area even though the tactical situation or supported units operating in the area may change. (See figure 4-1.)

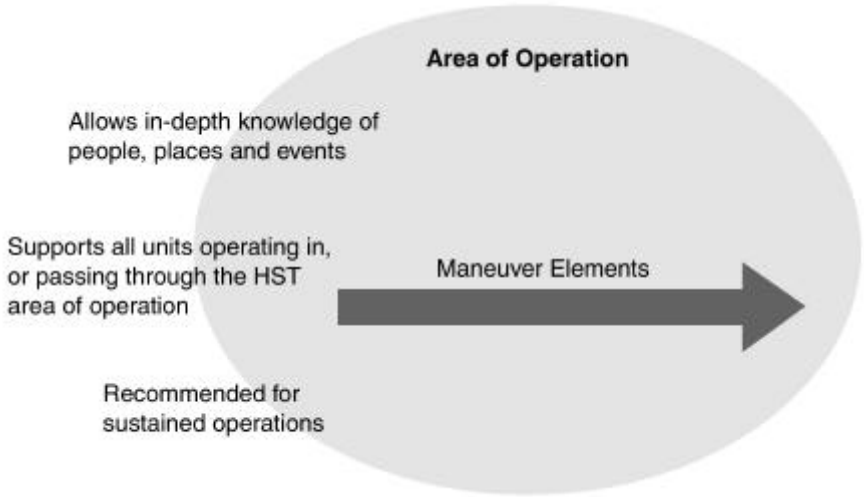

Figure 4-1. CI/HUMINT Support Using Area Coverage.

Continuity. Area coverage provides the greatest continuity of tactical CI operations. It allows MAGTF CI operations to focus on the enemy's intelligence organization and activities while remaining unfragmented and unrestricted by the tactical areas of responsibility assigned to support units. It also allows MAGTF CI personnel to become familiar with the area, enemy intelligence organization and operations, and CI targets. Area coverage is particularly effective during MOOTW (e.g., counterinsurgency operations) where the threat forces often operate on political, vice military, boundaries.

Unit Assignment

MAGTF CI elements employed on a unit assignment basis normally remain with designated supported units. They operate within that unit's AOR under the specified C2 relationships. As tactical units displace, it is necessary for higher echelons to provide CI coverage for the areas vacated. Relief of an area can be accomplished by three methods—attachment, leapfrog system, and relay system.

Attachment. CI elements may be detached from the MAGTF CE and attached to subordinate commanders. This method provides dedicated CI support under the operational control of the commanders to which the CI elements are attached for employment against specific CI targets during the initial (and possibly subsequent) phase of an operation. It also prepares for subsequent transfer of areas of responsibility from subordinate units to MAGTF CE without loss of continuity. These CI elements generally operate under the operational control of the supported commander during the initial reduction of CI targets. The CI elements then remain in place as the unit advances, reverting to the operational control of the MAGTF commander (or other specified commander) or intel bn commander. By remaining in place, the CI element ensures continuous coverage regardless of tactical unit movements.

Leapfrog System. This method is similar to the area coverage concept but on a smaller scale. Under the leapfrog system, MAGTF CI elements initially

responsible for a specified area are detached from subordinate units and a new team attached as the operation progresses. The new CI element is attached sufficiently in advance to permit it to become thoroughly familiar with current operations within the AOR. This method of relief permits the CI element familiar with the area, informants, and targets to remain and conduct more extensive operations, while providing necessary CI direct support to subordinate commanders.

Relay System. This method requires MAGTF CI elements to be held in reserve. As the subordinate units advance, CI elements are dispatched forward to assume control of designated areas on a rotational basis.

CI Employment Considerations

Characteristics of the AOR influence the nature and extent of MAGTF CI operations. The following factors influence CI task organization, C2, and resulting concepts of operations and support relationships.

- Historical and recent espionage, sabotage, subversion or terrorism activities within the AO.
- Population density.
- Cultural make-up of the civilian population.
- Attitude of the people and political groups toward friendly and enemy forces.
- People's susceptibility to enemy penetration (hostile intelligence threat) and propaganda.
- Stability of the local government, security, and law enforcement.

The number of MAGTF CI resources available, particularly HSTs, is critical. Careful planning, awareness of CI operations throughout the joint AOR, and detailed intelligence and operations preparation are required. CI targets that require early reduction must be selected and the employment of MAGTF CI operations planned. Care must be taken to not overestimate CI element capabilities-this risks overextending and dispersing CI activity on many targets with limited effectiveness.

During amphibious operations, the commander, landing force (CLF) assumes operational control over assigned CI assets. Clear responsibility for CI operations must be assigned among MAGTF, naval, and other supporting CI elements. CI investigations of a GS nature, particularly in rear areas, may be tasked to NCIS or other supporting CI elements. In such cases, jurisdiction must be clearly defined to optimize overall CI support.

Employment of MAGTF CE CI Elements

MAGTF CE CI elements normally operate in the rear area conducting the following tasks:

- Provide overall MAGTF CI operational management and technical direction.
- Coordinate and integrate of MAGTF CI operations with JTF, multinational, and other supporting CI operations.

- Conduct CFSO and HUMINT operations of a relatively long-term nature.
- Provide assistance on military and civil security matters.
- Follow-up and complete CI tasks initiated by subordinate elements.

The MAGTF commander normally retains OPCON over technical surveillance countermeasures, CI inspections, and CI surveys for the entire MAGTF, which are exercised via the G-2/S-2 and the ISC. If required, intel bn may also establish and operate the MAGTF CI interrogation center.

Employment of CI Elements with the Ground Combat Element

Generally, the number of MAGTF CI elements employed in the ground combat element (GCE) AOR is greater than in other areas. During combat and in enemy occupied areas, the enemy has more opportunities to penetrate the CI screen because of the constant contact of opposing ground forces and the presence of indigenous or displaced populations. After the area has been cleared of the enemy, the CI element operating with the GCE is usually the first security unit to enter this area. They help determine initial requirements and establish initial security measures. CI elements with the GCE perform critical preparatory tasks for all subsequent CI and security operations. Prompt action by CI elements, particularly the rapid development and dissemination of intelligence based on interrogations or exploitation of captured materials and documents, can be of substantial benefit to the GCE's operations and force protection efforts.

The CI element focuses its operations on the GCE's distant and close areas, with responsibility for GCE rear area generally being coordinated with CI elements operating in GS of the MAGTF or those in direct support of the rear area operations commander. The CI elements operating with a division are generally deployed by task organizing multiple HSTs, although employment of CI teams is also an option. The HSTs and CI teams are responsible for the CI coverage of specific areas within the jurisdiction of the command. Each HST or CI team acts as an independent unit, but its activities are coordinated by the CI/HUMINT Company Commander or by one of the team OICs.

Time is essential during the initial phase of an operation. CI elements employed with attacking forces will generally limit their screening operation to identification and classification of enemy agents, collaborators, and civilians disguised as military personnel. If time permits, immediate tactical interrogation may be conducted of suspects. Normally, suspects will be passed to rear area, intermediate detention facilities, ultimately arriving at the Joint Interrogation and Debriefing Center for more detailed interrogations and classification.

CI elements must identify and secure—

- The most obvious CI targets.
- Agents left behind by the enemy for espionage and sabotage.
- Enemy collaborators.
- Key public buildings, such as the seat of the local government, police stations and communication centers.

Employment of CI with the Aviation Combat Element

There is no significant difference in the mission of CI elements employed with either ground or air units. However, air units are normally characterized

by a static position. CI elements or personnel are attached or placed in GS of the tactical command echelon(s). They advise the commander on the control and security of sensitive areas, civilian control measures, and screening of local residents and transients. They also assist with the conduct of security assessments of facilities in the vicinity as required.

The aviation combat element (ACE) is often widely dispersed with elements operating from separate airfields. Since aircraft and support equipment are highly susceptible to damage and difficult to replace, aviation units are high priority targets for enemy saboteurs and terrorists. In many situations, ACE units employ large numbers of indigenous personnel in support roles, personnel who are a key target of enemy intelligence activities. Under such conditions, it may be necessary to provide HSTs in direct support of ACE elements.

CI Support to the Combat Service Support Element and Rear Area Operations

Within rear areas, the MAGTF CSSE is generally the principal organization requiring CI support. While the combat service support element's (CSSE) CI requirements are primarily concerned with military security, those of civil affairs elements generally deal with civil/military interaction and security of the populace. Despite the apparent differences of interest between their requirements, their CI problems are interrelated (e.g., a dissident civilian population hampering the efforts of MAGTF civil affairs elements attempting to establish effective administrative control in the area also disrupting logistics operations through sabotage, terrorism, and harassment attacks).

MAGTF CE CI elements performing GS to CI operations normally provide CI support to CSSE and other rear area operation elements. This includes support for installations and facilities dispersed through the combat service support areas. The number of team personnel supporting civil affairs units depends on the number of refugees to be identified in the area.

4003. FRIENDLY PRISONERS OF WAR AND PERSONS MISSING (NON-HOSTILE) AND MISSING IN ACTION

Friendly personnel who are captured by the enemy can be a source of information through the compromise of documents, personal papers or as the result of effective interrogation or coercion. It is a fundamental command responsibility to take necessary steps to counter any possible disclosure that would affect the immediate tactical situation.

CI units are assigned responsibility for investigating and determining risks posed to MAGTF operations by friendly personnel who have or may have been captured. They will help collect information of potential intelligence value on friendly personnel who may be under enemy control. They also collect intelligence information to aid in identifying, locating, and recovering captured friendly personnel. In addition, CI personnel conduct

the intelligence and CI debriefings of friendly personnel who had been captured and then returned to friendly control.

When friendly personnel have or may have been captured, the identifying commander will immediately notify their unit intelligence officer, who will then coordinate with the pertinent CI element to initiate the CI investigative process (see appendix D). The CI unit may be able to immediately provide information that could aid in the search and recovery efforts, such as routes to enemy detention centers, locations of possible holding areas, and enemy procedures for handling and evacuating prisoners. If appropriate, the CI element can also initiate immediate CI collection action, such as using CI sources to gain information for possible recovery or search and rescue operations.

If the search or recovery attempts are unsuccessful, the CI unit initiates an immediate investigation to gather basic identification data and determine the circumstances surrounding the incident.

The investigation must be as thorough and detailed as possible and classified according to content. Every attempt is made to obtain recent photographs and handwriting samples of the captured person. A synopsis of the investigation, including a summary of the circumstances, is prepared on the CI report form. The completed basic identifying data form is attached as an enclosure to this report.

In the case of aircraft incidents, the investigation includes type of aircraft, location, and sensitivity of classified equipment, bureau or registration number, call signs, and any aircraft distinguishing marks, such as insignia, etc. When feasible, the investigator should coordinate with the accident investigation team or aviation safety officer of the unit that experienced the loss.

The investigation is designed to—

- Provide information to aid in subsequently identifying and locating the individual.
- Assess the potential intelligence value to the enemy.
- Collect intelligence information that will be of value when evaluating future intelligence reports.

The CI report, with the attached personnel data form, is distributed to the following commands:

- MARFOR component HQ, the MAGTF CE, and intel bn/detachment.
- Individual’s parent command (division, Marine Aircraft Group or Force Service Support Group).
- Each CI element in the AOR.
- Other appropriate headquarters (e.g., combatant commander, Marine Corps Forces (MARFOR) headquarters, etc.).
- CMC (Counterintelligence Branch).

These reports are designed to aid follow-on CI operations. They do not replace normal G-1/S-1 casualty reporting procedures. When the CI report concerns a member of another Service assigned to a Marine Corps unit, a copy of the report is also provided to the appropriate component commander and Service headquarters. Subsequent pertinent information is distributed in the same manner as the initial CI report.

CI personnel debrief personnel returned to friendly control after being detained by the enemy. Normally, CI personnel supporting the unit that first

gains custody of the individual conduct an initial debriefing to identify information of immediate tactical value and the locations of other friendly prisoners of war. As soon as possible, the returnee is evacuated to the MAGTF CE for further debriefing and subsequent evacuation to a formal debriefing site.

4004. UNIQUE CI SUPPORT DURING MOOTW

The CI operations previously discussed are generally applicable across the spectrum of MOOTW, including non-combatant evacuation, peace, and humanitarian and disaster relief operations. CI activities during MOOTW require CI personnel to be thoroughly familiar with the nature of operation, including its causes, characteristics, peculiarities, and with the threat infrastructure directing and controlling enemy efforts. Basic CI tasks are the denial of information to the threat force and the identification and neutralization of intelligence operations. A key aim of MOOTW is to restore internal security in the AOR, which requires a vigorous and highly coordinated CI effort.

Jurisdiction

The nature of the operation and the threat's covert methods of operation require the employment of a greater number of CI personnel than is generally required for conventional operations.

Effective CI operations require extensive coordination with the host country intelligence, CI, security, and law enforcement agencies. Operations are normally covered by a status of forces agreement (SOFA). A SOFA may include limitations and restrictions concerning the investigation and apprehension of host country citizens or other operations matters.

MAGTF CI Employment

Employment of CI elements during MOOTW is similar to that previously described. CI area coverage generally provides continuity of operations. As the threat's intelligence operations usually are well established, area coverage allows MAGTF CI personnel to better understand and more effectively counter the threat.

When assigning AORs, MAGTF CI elements ensure coverage overlaps to preclude gaps occurring between areas. Threat forces usually prefer to operate on the political or military boundaries where the assigned responsibilities of U.S. and allied forces may be vague and coordination is more difficult. CI elements employed through unit assignment are assigned responsibility for the area of interest around specified unit's area of responsibility. Under the unit assignment concept, rear area CI elements assume responsibility for any gap in coverage that may develop.

CI Measures and Operations

MOOTW usually require both passive and active CI measures be increased and aggressively pursued to effectively counter the threat's advantages and capabilities.

MAGTF units must institute and continuously enforce CI and security measures to deny information to the threat force and to protect friendly units from sabotage, espionage, subversion, and terrorism. In coordination with host country authorities, emphasis is needed on security measures and checks of indigenous employees or other persons with access to MAGTF installations, facilities, and command posts.

A significant factor during MOOTW is population and resources control. The movement channels and patterns necessary for support, communications, and operations of insurgent forces are observed and controlled. Prior to implementing control measures, the civilian population should be informed of the reasons for the controls. Whenever possible, such controls should be performed and enforced by host country agencies.

Basic CI operations, techniques, and procedures are generally applicable during MOOTW.

MAGTF CI elements must implement imaginative and highly aggressive special CI operations and HUMINT collection programs targeted against the threat's intelligence infrastructure and operational forces. The primary objective of special operations is the identification, location, and neutralization of specific members of the threat's infrastructure. A CI special operation consists of systematic intelligence collection and analysis with complete documentation concerning the activities of each targeted individual. This provides the host country with an account of the individual's illegal activities once the person is apprehended. Penetration of the infrastructure must be achieved at all levels possible—HUMINT operations are implemented to cover critical areas and to identify and locate threat forces. Intelligence derived from HUMINT programs may also be useful in CI special operations.

Cordon and search operations basically consist of—

- Security forces that surround the area, usually at night, to prevent persons from leaving the area.
- A sweep element that escorts detained people to a collection point at first opportunity.
- Search elements that conduct detailed en-mass searches of the area.
- Screening elements to process and screen detainees for identification of known or suspected threat personnel.

In MOOTW, cordon and search operations may be employed to ferret out the threat infrastructure. Ideally, a cadre of MAGTF CI personnel are assigned to each unit conducting the cordon and search operation to provide on scene exploitation and immediate reporting of threat related time-sensitive intelligence. These operations may also be employed to ferret out individual threat units that may use a community or area as cover for their activities or as a support base. Cordon and search operations should be conducted with host country forces and organizations, with U.S. forces including CI units providing support, advice, and assistance for the operation. At a minimum, host country personnel should be part of the screening and sweep elements of any cordon and search operation. Sweep/screening is often conducted with medical, civil affairs, and psychological operations programs that are accomplished after the screening phase. Throughout the operation, care must be exercised to prevent an adverse psychological effect on the populace.

CHAPTER 5. C2 AND CIS SUPPORT TO MAGTF CI OPERATIONS

5001. GENERAL

The MAGTF CI effort depends heavily on secure, reliable, and fast communications and information systems (CIS) support to receive JTF, other components, theater, and national CI and all-source intelligence and to transmit organically collected and produced CI product and reports. CIS are also required for the command and control of MAGTF and supporting CI units and their integration with other intelligence and reconnaissance operations. Every mission and situation is unique, requiring some modifications to the supporting CIS architecture to support MAGTF CI operations. Detailed planning and close coordination between the CI/HUMINT company/detachment CO/OICs, the MAGTF G-2/S-2 and G-2/S-6, and pertinent operational and intelligence organizations is critical for establishing a reliable and effective CI CIS support.

See MCWP 6-22, *Communications and Information Systems*, for a detailed review of MAGTF CIS doctrine and supporting tactics, techniques, and procedures.

5002. COMMAND AND CONTROL

JTF J-2 and the Joint Intelligence Support Element

General

The JTF J-2 organizational structure and capabilities will be situation and mission dependent as determined by the JFC and the JTF J-2. The JISE is the principal intelligence C2 node within the JTF J-2. The JISE is the focus for JTF intelligence operations, providing the JFC and component commanders with situational awareness and other intelligence support regarding adversary air, space, ground, and maritime capabilities and activities. CI collection, production and dissemination activities will be conducted within the JISE, or within the J-2's joint force J-2 CI/HUMINT staff element (J-2X), if established. Once initial basic and current CI products and support have been provided to the JTF and its components, updates will be accomplished by the JISE using push/pull dissemination techniques. Intelligence CIS based on the JDISS/Joint Worldwide Intelligence Communications System (JWICS) functionality provide the JTF with the ability to query theater and national CI organizations' servers and data bases for the most current CI support.

J-2X

Joint force commanders have operational control of JTF CI elements not organic to its component commanders, which they exercise via the JTF intelligence officer (J-2). Within the J-2, CI activities fall under the functional control of the TFCICA and HOC, which comprise the intelligence section's J-2X. CI collection operations management, CI production and CI dissemination tasks are exercised by the TFCICA, to include source deconfliction with the Central Source Registry, reporting coordination and resource application. Other functional managers, such as the Defense HUMINT Service representative within the J-2X or the HOC, have direct

tasking authority over their functional assets, requiring close coordination and planning to ensure effective JTF CI/HUMINT operations.

National Intelligence Support Team

All-source national intelligence level CI and other intelligence assets may deploy in support of JTF (and even directly in support of MAGTF) operations to provide critical support via reach back and collaborative intelligence capabilities. The national intelligence support team (NIST) is the most typical method used. Its mission is to provide a tailored, national level all-source intelligence team to deployed commanders (generally at the JTF headquarters level, but support could be provided to other commands) during crisis or contingency operations. Depending on the supported unit's requirements, a NIST can task-organize to provide coordination with national intelligence agencies, analytical expertise, I&W, special assessments, targeting support, streamlined and rapid access to national intelligence data bases and other products, and assistance facilitating RFI management (see figure 5-1).

The NIST is a task-organized unit generally consisting of DIA, National Security Agency, Central Intelligence Agency, and, as appropriate, National Imagery and Mapping Agency personnel and equipment.

DIA, through the joint staff J-2, controls the NIST for deployment and administrative purposes. The composition and capabilities of each NIST deployment are unique based on the mission, duration, agencies representation, and capabilities required (see figure 5-2). During operations a NIST will usually be in direct support of the JFC, who exercises C2 via the JTF J-2. If a NIST is provides support of the JTF HQ, it generally will integrate its operations within the JISE. Key JISE functions and capabilities include collection management support, order of battle (OOB) analysis, identification of threat centers of gravity and critical vulnerabilities, and intelligence support to targeting and force protection.

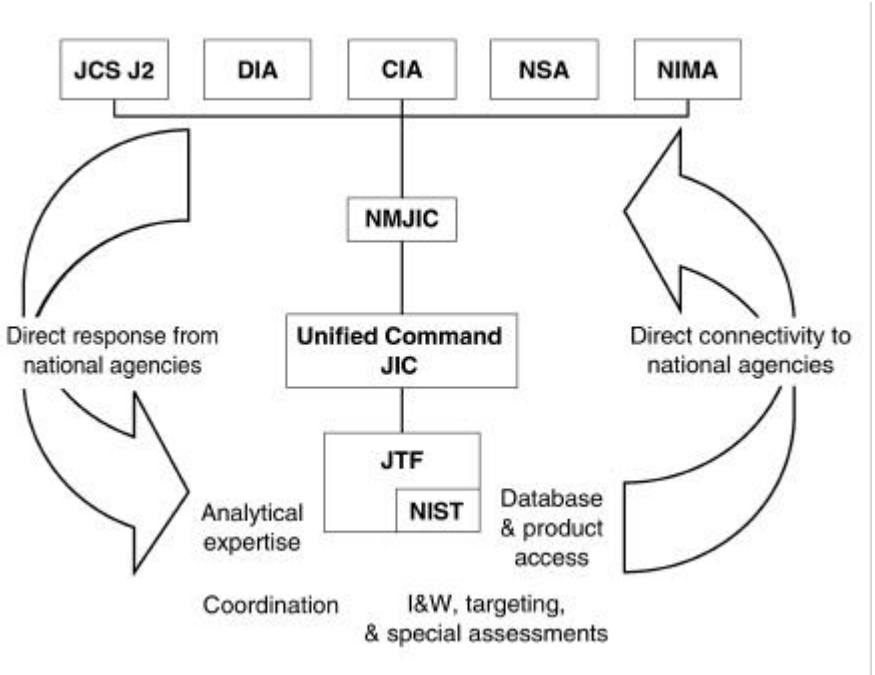

Figure 5-1. National Intelligence Support Team Capabilities.

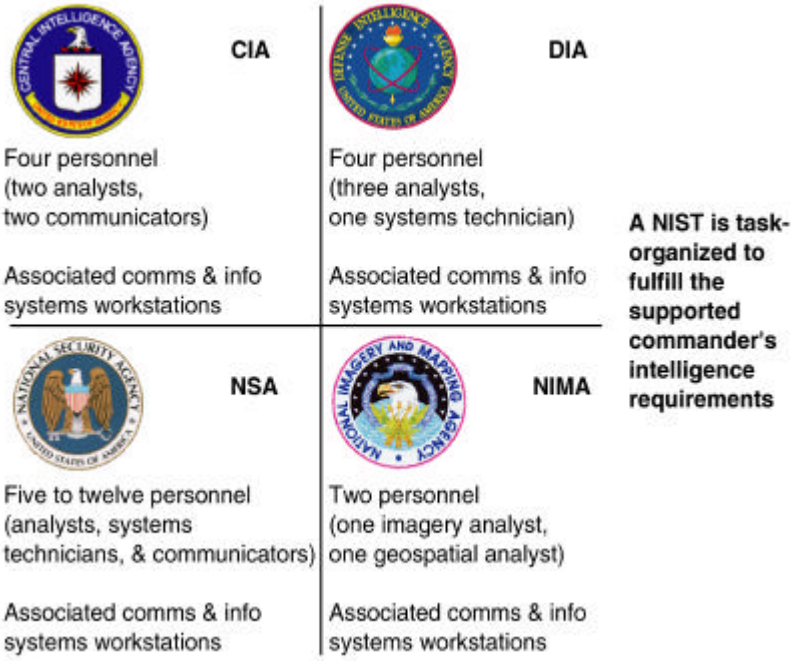

Figure 5-2. Notional Composition of a National Intelligence Support Team.

Once deployed, any of the intelligence agencies with representatives on the NIST can provide its leadership. The basic C2 relationship between the NIST and the JTF (or other supported commands) is direct support. The NIST will be under the staff cognizance of the JTF J-2, performing intelligence support functions as so designated. The basic NIST concept of operations is to take the J-2's RFIs and collection and production requirements, discuss and deconflict these internally within the NIST to determine which element(s) should take these for action. Each NIST element leader, coordinated by the NIST team chief, will conduct liaison with their parent national intelligence organization. Intelligence and CI generated by the NIST will be disseminated to the JTF J-2 JISE or J-2X, the JFC, and other components of the JTF with the usual restriction based on clearance and programs.

A NIST's organic capabilities generally encompass only intelligence and some unique CIS support. NIST CIS capabilities will be task-organized. It may range from a single agency element's voice connectivity to a fully equipped NIST with joint deployable intelligence support system (JDISS) and Joint Worldwide Intelligence Communications System (JWICS) video teleconferencing capabilities (see figure 5-3 on page 5-4 for one of a NIST's key sophisticated CIS capabilities). Current methods of operation continue to rely on both agency and supported command-provided communications paths to support deployed NIST elements. The systems that elements are capable of deploying are discussed in greater detail in appendix C, NIST Systems, of JP 2-02, *National Intelligence Support to Joint Operations*.

Figure 5-3. NIST JWICS Mobile Integrated Communications System.

Amphibious Task Force Intel Center

During amphibious operations, amphibious task force (ATF) and the MEF CE's intelligence sections generally will integrate their operations. The principal intelligence C2 node is the amphibious task force intel center (ATFIC) located aboard the ATF flagship. The ATFIC is composed of designated shipboard spaces with installed CIS that support the intelligence operations of both the ATF and landing force while reducing duplicative functions and producing more comprehensive and timely intelligence support for the naval task force. Standard CIS connectivity is available—JWICS, SECRET Internet protocol router network (SIPRNET), nonsecure Internet protocol router network (NIPRNET), AUTODIN, DSN. Access is provided via the flagship's GENSER communication center and the special intelligence communications center within the ATFIC's ship's signals exploitation space.

MEF Command Element Intelligence C2 and Operations Nodes

Combat Intelligence Center and Intelligence Operations Center

The CIC and its subordinate elements is the principal MAGTF intelligence C2 node that provides the facilities and infrastructure for the centralized direction for the MEF's comprehensive intelligence, CI and reconnaissance operations. Since the CIC must effectively support the MEF, it must remain responsive to the requirements of all elements of the MAGTF. In supporting this objective, the CIC integrates and supports both MEF G-2 section and intel bn operations. While integrated, the organizational approach differs some for each of these.

CIC—overarching intelligence operations center established within the MEF main command post. Encompasses the primary functions of the MEF intelligence section and intel bn. It includes the sub-elements listed below.

G-2 Plans—main element of the G-2 section for coordinating and providing intelligence support to the MEF CE future plans team; and leadership and direction of the G-2 section's imagery and mapping, SIGINT, and weather sections.

G-2 Operations—main element of the G-2 section for coordinating and providing intelligence support to the MEF CE CG, battle staff and current operations center elements; target intelligence support to the force fires and future operations; G-2 section intelligence requirements management activities; Red Cell support; and MEF intelligence liaison with external commands and organizations.

IOC—principal MEF intelligence operations and C2 center that is established by intel bn. Performs intelligence requirement management, staff cognizance of ongoing organic and supporting collection operations, intelligence analysis and production, and intelligence dissemination.

- **Support Cell**—primary element for conducting MEF-wide intelligence requirements management; weather support; collections and dissemination planning and direction; and intelligence staff cognizance of MEF organic and supporting intelligence and reconnaissance operations.
- **P&A Cell**—primary analysis and production element of the MEF. Processes and produces all-source intelligence products in response to requirements of the MEF. It is the principal IMINT and GEOINT production element of the MEF.
- **Surveillance and Reconnaissance Cell (SARC)**—primary element for the supervision of MEF collection operations. Directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets.
- **CI/HUMINT Company Command Post**—primary element for conducting CI/HUMINT planning and direction, command and control, and coordination of MEF CI/HUMINT operations with external CI/HUMINT organizations.

Operations Control and Analysis Center (OCAC)—main node for the C2 of radio battalion SIGINT operations and the overall coordination of MEF SIGINT operations. Processes, analyzes, produces, and disseminates SIGINT-derived information and directs the ground-based electronic warfare activities of the radio battalion.

Reconnaissance Operations Center (ROC)—main node for the C2 of force reconnaissance company's operations and the overall coordination of MEF ground reconnaissance operations. Processes, analyzes, produces, and disseminates ground reconnaissance-derived information in support of MEF intelligence requirements.

G-2 Section

The key G-2 nodes are organized to effectively align and support the MEF CE's staff cross-functional cellular staff organization and concept of operations. The G-2 plans branch provides intelligence and CI support to the MEF CE's future plans cell efforts. The G-2 operations branch, provides intelligence and CI support to the MEF CE's COC, FOC, force fires center

and directs and manages the G-2's Red Cell and the MEF's external intelligence liaison teams (see figure 5-4).

CIC facilities, CIS, and other support must allow the AC/S G-2 and G-2 section to perform the following major tasks:

- Develop and answer outstanding MEF and subordinate units' PIRs and IRs by planning, directing, integrating, and supervising MEF organic and supporting intelligence, CI and reconnaissance operations.
- Plan the MEF concept of intelligence operations, including a concept for CI operations, for approval by the AC/S G-2 and subsequent implementation by the ISC based upon the mission, threat, commander's intent, guidance, and concept of operations.
- Recommend CI and force protection measures and countermeasures.
- Prepare appropriate intelligence and CI plans and orders for the MEF, including reviewing, coordinating, and integrating the intelligence plans of JTFs, theaters, and other organizations.
- Coordinate, provide, and facilitate the use of intelligence and CI to the MEF CG, the battlestaff, the future plans cells, the FOC, the COC, and the force fires center.
- Plan, direct, and supervise MEF liaison teams to external commands (e.g., the JTF and joint functional components headquarters) and intelligence organizations.
- Coordinate and supervise the transition of intelligence and CI planning and operations from G-2 plans to G-2 future operations, and from G-2 future operations to G-2 current operations, to effectively support the MEF's single battle transition process.

Intelligence Operations Center

The key subordinate elements within the IOC and their typical composition are the support cell, the SARC, and the P&A cell (see figure 3-3 on page 3-6).

The IOC is the other principal MEF CE intelligence node. It provides the facilities, CIS, and other support to allow the ISC and intel bn to perform the following tasks:

- Provide centralized direction for MEF intelligence and CI operations under the staff cognizance of the AC/S G-2. The IOC is the core for this task, with key assistance from the G-2 plans and G-2 operations elements.
- Consistent with the commander's priorities, consolidate, validate, and prioritize IRs of the entire force. The key CIC element providing for this is the collection management and dissemination (CMD) section within

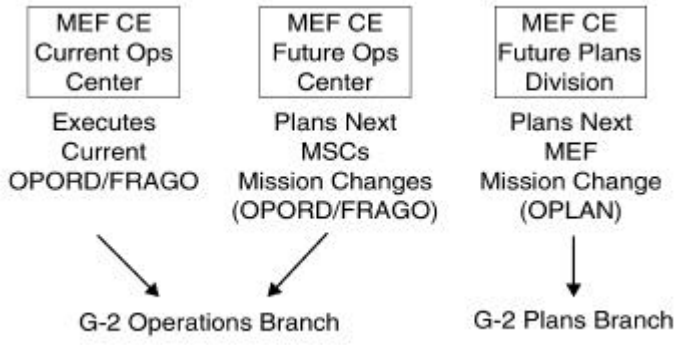

Figure 5-4. MEF CE Cross-Functional Cellular Organization and Intelligence Support.

the IOC's support cell. Intelligence specialists from all disciplines, including CI, generally are organic to this section.

- Plan, develop, and direct the MEF collection, production, and dissemination plans and operations. The key CIC elements providing for this are the CMD section within the IOC's support cell and the P&A cell.
- Submit consolidated requests for external intelligence and CI support through the Marine component headquarters to appropriate agencies. The key CIC element providing for this is the CMD section within the IOC's support cell, with assistance from the P&A cell and the G-2 operations branch.
- Allow the ISC to exercise, per AC/S G-2 cognizance, principal staff cognizance of MEF organic and supporting intelligence and reconnaissance operations, including CI, HUMINT, SIGINT, IMINT, GEOINT, measurement and signature intelligence (MASINT), ground reconnaissance, and aerial reconnaissance operations.
- Coordinate and manage the employment of MEF organic collection assets through the IOC's SARC. Within the SARC will be representatives from most organic and supporting intelligence, CI and reconnaissance units to provide C2 and reporting of ongoing intelligence operations.
- Maintain a consolidated, all-source intelligence production center in the MEF in the IOC's P&A cell. Other nodes with significant intelligence production involvement are the radio battalion's operations control and analysis center (OCAC) and the CI/HUMINT Co's CP. Similar to the CMD section, intelligence specialists from intelligence disciplines generally are organic to the P&A cell.
- Link the MEF CE to national, theater, joint, other-Service, and multinational intelligence and CI assets and operations. Intel bn, G-2 section C2, and operations nodes have common and unique capabilities to perform critical tasks within the function. In addition to MEF CE common communications pathways provided by the communications battalion, the IOC generally will also have unique intelligence communications capability, such as Trojan Spirit II.

Overall MEF Intelligence C2 Relationships

The MEF G-2 section and intel bn's overall command and control relationships and resulting all-source intelligence support flow throughout the MEF are as indicated in figure 5-5 on page 5-8.

CIC/IOC Operations and MAGTF CI Operations

Key CI activities, which will be integral to many CIC/IOC operations, include—

- **Collection.**
  - The CMD section, HQ, Intel Bn, provides the core for MEF CIC collection operations. During operations the CMD section is located within the IOC's support cell. Intelligence specialists from all disciplines, including CI, are organic to this section. Key CIS resources required include intelligence analysis system (IAS) and access to the full range of communications: (JWICS, SIPRNET, NIPRNET, DSN, etc.).
  - The SARC, another key element within the IOC, provides the other key component of collection operations. Within the SARC will be representatives from most organic and supporting intelligence

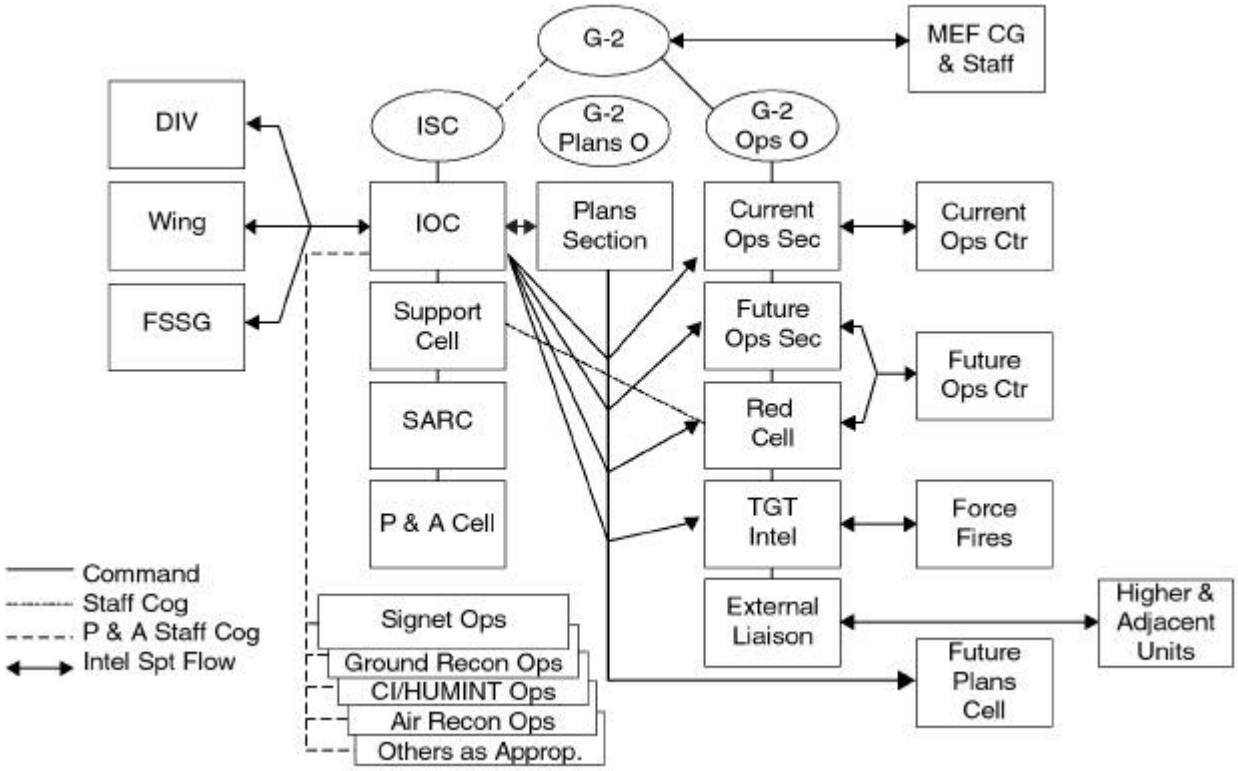

Figure 5-5. MEF G-2 and Intelligence Battalion C2 Relationships and MEF Intelligence and CI Support Flow.

and reconnaissance units providing C2 and reporting of ongoing intelligence operations. Regarding CI, the SARC will include representatives from CI/HUMINT Co to monitor ongoing CI/HUMINT operations and report time-sensitive intelligence.

- **Production.** The P&A cell, Intel Bn, provides the core for MEF intelligence production operations. Similar to collection, intelligence specialists from all intelligence disciplines are organic to the P&A cell. Key CIS resources required include IAS and JDISS, with access to the full range of communications (JWICS, SIPRNET, NIPRNET, DSN, etc.). Additionally, the operations/analysis element from CI/HUMINT company may be integrated into P&A cell operations to efficiently support both CI and all-source production operations.
- **Dissemination.** The CMD section, HQ, Intel Bn, provides the core C2 for MEF intelligence dissemination operations. Key CIS resources required include IAS and JDISS, with access to the full range of communications (JWICS, SIPRNET, NIPRNET, DSN, etc.) for external dissemination; and IAS via the TDN and other MEF communications resources for internal dissemination.

CI/HUMINT Company HQ

CI and IT platoons elements as well as task-organized HSTs generally will be employed throughout MAGTF. To support operations, the CI/HUMINT company headquarters will usually establish a command post (CP) in the vicinity of the IOC, integrated with and employing the full range of CIS supporting it.

CI/HUMINT Co C2, planning and direction, and some analysis, production, and dissemination functions are executed within the CI/HUMINT Co CP. The CI/HUMINT Co personnel within the CP perform the CI and HUMINT processing, analysis, exploitation, production, and reporting of CI and HUMINT products and information per ISC direction and the intelligence operations plan.

It is the principle element that coordinates with other intel bn and G-2 nodes to plan and direct CI/HUMINT operations.

Deployed CI/HUMINT Elements

CI/HUMINT elements—HSTs, CI teams, IT teams—will generally be deployed at many command echelons and locations within the MAGTF. For example, significant elements may be attached or placed in direct support of GCE forces or the rear area operations commander. Likewise, CI/HUMINT elements may be employed at the MAGTF EPW compound and other EPW collection points. The CIS resources used by these CI elements will be dependent upon the situation. Generally these elements will use company or intel bn CIS resources to satisfy their organic C2 needs, while using the supported unit's CIS resources for broader requirements.

5003. BASIC CI CIS REQUIREMENTS

Regardless of the size of MAGTF CI/HUMINT forces, there are certain standing CI CIS requirements must be satisfied. These requirements are—

- **Capability to command and control subordinate units.** Intelligence officers and CI/HUMINT element commanders/OICs must be capable of positive C2 of subordinate units and integration of its operations with broader MAGTF and external intelligence and operations C2. Traditionally single-channel radio and record message traffic have been used to support C2 of MAGTF CI units. In semi-static situations, secure E-mail or telephone may be the method of choice, while in highly fluid or mobile scenarios, cellular, SATCOM, and VHF and HF radio may be used.
- **Ability to receive collected data and information from deployed CI elements.** The CIS architecture must provide connectivity between organic and supporting CI/HUMINT elements (such as the HUMINT support teams or CI liaison elements), CI analysis and production centers, and supported MAGTF operations and intelligence centers. Requirements include the capability to transmit collection files and reports digitally via fiber optics, wire, or radio in formats (both voice and data) that are readily usable by the CI and all-source intelligence analysts.
- **Ability to provide intelligence to supported commanders.** CI CIS requirements will be influenced by supported commanders' intents, concepts of operations and intelligence, command relationships, and standing PIRs and IRs. The CIS architecture must be capable of integrating CI/HUMINT element C2 and supporting CIS operations (including special communications capabilities and channels unique to CI reporting) with the primary CIS channels used by supported commanders.
- **Ability to share CI products and reports with MAGTF all-source intelligence centers and with CI and all-source JTF, other components, theater, and national CI and intelligence centers.** The traditional means for providing this capability are MAGTF general service secure record and voice communications. While these techniques

continue to be used, they are rapidly becoming secondary in importance to the use of the JWICS, the SIPRNET, and CI unique CIS capabilities that allow participants to access each others CI products and data bases and immediately pull required data, intelligence, and CI products.

5004. CIS SUPPORT TO MAGTF CI OPERATIONS

General

CI CIS architecture for any given operation is dynamic. Key reference documentation with respect to a specific theater or MAGTF operation are—

- Combatant command, JTF, and MAGTF CI/HUMINT plans developed for various OPLANs.
- MAGTF command element intelligence SOP and combatant commanders intelligence and CI/HUMINT tactics, techniques, and procedures.
- Annexes B (intelligence), C (operations), J (command relationships), and K (communications and information systems) of the MAGTF and JTF OPORDs.
- The following parts of Annex B (Intelligence) to a MAGTF OPORD: Appendix 3 (Counterintelligence Operations); appendix 5 (Human Resources Intelligence Operations); and tab D (Intelligence Communications and Information Systems Plan) to appendix 16 (Intelligence Operations Plan).

Communications Systems

Information systems and supporting communications connectivity are evolving rapidly within the Marine Corps and other elements of the military. The following information provides typical key MAGTF CI communications requirements.

The MAGTF mission, the nature of the threat, friendly concepts of operations and intelligence, supporting task organization and command relationships, and extent of allied/ multinational operations are the key factors influencing what specific CI communications are established during operations.

Intelligence and CI/HUMINT Radio Nets

The following are radio nets typically established for either dedicated CI needs or are intelligence nets that CI elements may need to be stations on:

MAGTF Intelligence (UHF-SATCOM/HF/VHF). Used for rapid reporting and dissemination of intelligence, collaborative planning of future MAGTF intelligence operations, and C2 of ongoing MAGTF intelligence and reconnaissance operations. Typical organizations/elements participating in this net include: the MAGTF CE; the GCE/ACE/CSSE headquarters; intelligence, CI and reconnaissance elements either attached to, OPCON or supporting the MAGTF; and others as directed.

GCE/ACE/CSSE Intelligence (HF/VHF). Used to provide rapid reporting and dissemination of intelligence, collaborative planning of future intelligence operations, and command and control of ongoing intelligence and reconnaissance operations. Typical organizations/elements participating in this net include: the GCE/ACE/CSSE headquarters; headquarters of their major subordinate units; intelligence, CI and reconnaissance elements either attached to, OPCON or supporting the MSE headquarters; and others as directed.

CI/HUMINT Team(s) Command (HF/VHF). Used for C2 of CI teams, IT teams, and HSTs operations, and the coordination of CI/HUMINT administrative and logistic support. This net will also generally terminate in the MAGTF SARC.

CI/HUMINT Reporting Net (VHF/HF). Used as a means for the rapid reporting of CI/HUMINT data to supported units. Participants generally include CI teams, IT teams, and HSTs operations, the SARC, and the intelligence centers of any supported units.

CI/HUMINT Communications Equipment

CI elements require extensive communications support from the command to which they are attached. These requirements include secure dedicated and shared systems connectivity and are situationally dependent based upon employment method, terrain, distance, and other factors. CI elements usually deploy with the following organic communications and information systems:

- **SINCGARS radios**—primarily to support CI element C2 and intelligence reporting.
- **Motorola SABER radios**—principally to support internal CI element communications of an operational nature (e.g., surveillance or security).

The command provides frequency management, cryptographic materials system control, and logistics support (e.g., batteries and maintenance).

Intelligence and CI/HUMINT Information Systems

The following systems and data bases are established for either dedicated or multipurpose use.

Joint Deployable Intelligence Support System

JDISS is an all-source automated intelligence tool that provides the backbone of intelligence connectivity among the national, theater, JTF headquarters, component commanders, and other intelligence organizations. JDISS employs a transportable workstation and communications suite that electronically extends JIC capability to a JTF and other tactical users. SIPRNET or JWICS will provide the principal communications connectivity for JDISS.

Intelligence Analysis System

IAS provides automated applications and other tools for MAGTF all-source intelligence planning and direction, management, processing and exploitation, analysis and production, and dissemination. Various configurations of IAS will be organic to intelligence sections from the battalion/squadron through MEF CE levels.

Defense Counterintelligence Information System

Defense counterintelligence information system (DCIIS) is a DOD system that automates and standardizes CI functions at command echelons. DCIIS contains standardized DOD forms (for CI investigations, collections, operations, and analysis and production) and shared CI data bases. DCIIS also contains supplemental forms to satisfy tactical reporting requirements

of Marine and Army CI elements. DCIIS is interoperable with JDISS and other intelligence systems.

Defense Intelligence Threat Data System

Defense intelligence threat data system (DITDS) is available via JDISS, IAS and other intelligence systems. It contains the DOD CI/counter-terrorism/ counter-proliferation data bases and is principally used by CI analysts and production personnel. The system provides a number of analytical tools, such as automated and graphical link analysis hot-linked to the underlying reports, automatic time lining and access to various communications systems to support dissemination. Communications connectivity is via SIPRNET

Migration Defense Intelligence Threat Data System

Many of the current intelligence/CI data bases that reside on other systems will become resident within the MDITDS. Some of these include DITDS, SPHINX (DIA's CI data base), CANNON LIGHT (U.S. Army CI data base), BLOODHOUND (EUCOM CI data base), Automated Intelligence Information Retrieval System, Automated Decisionmaking and Program Timeline, Defense Automated Warning System, Sensitive Compartmented Automated Research Facility, Terrorism Research & Analysis Program (TRAP), and many others.

The migration defense intelligence threat data system (MDITDS) is being developed to operate on the DCIIS to provide an automated production system for DODIIS I&W, CI, counterterrorism, and Arms Proliferation/ Defense Industry communities.

HUMINT Operational Communications Network

HUMINT operational communications network (HOCNET) is the umbrella name given to a collection of systems and applications currently operational or under development that support the Defense HUMINT Service (DHS) worldwide activities (i.e., Defense Attaché Worldwide Network).

Special Operations Debrief and Retrieval System

Special operations debrief and retrieval system (SODARS) provides detailed mission debriefs and after-action reports from special operations forces (SOF). As SOF are often the first and perhaps only DOD force committed to an operation, they may provide invaluable intelligence and CI when developing pre-deployment threat assessments.

AN/PYQ-3 CI/HUMINT Automated Tool Set

AN/PYQ-3 CI/HUMINT automated tool set (CHATS) consists of CIS hardware and software designed to meet the unique requirements of MAGTF CI/HUMINT elements. Operating up to the SECRET level and using the baseline DCIIS software suite, the system provides the capability to manage MAGTF CI assets and analyze information collected through CI investigations, interrogations, collection, and document exploitation. With CHATS, CI units may electronically store collected information in a local data base, associate information with digital photography, and transmit/receive information over existing military and civilian communications. (See appendix A for additional information on CHATS.)

Joint Collection Management Tool

Joint collection management tool (JCMT) is the principal automated tool for all-source intelligence collection requirements management. It provides a capability for management, evaluation, and direction of collection operations. Using DCIIS, CI collection requirements and taskings can be accessed from the JCMT.

Community On-Line Intelligence System for End-Users and Managers (COLISEUM) System

Community on-line intelligence system for end-users and managers (COLISEUM) is the automated, DOD intelligence production program requirements system that allows authorized users to directly submit multi-discipline intelligence production requirements to commanders and intelligence production centers. COLISEUM also tracks responses and provides status reports on validated production requirements.

Summary

Figure 5-6 on page 5-14 depicts a notional MEF CI architecture, and figure 5-7 on page 5-15 depicts key CI elements and supporting CIS within the MEF CE CIC and IOC. The three key aspects of MAGTF CI C2 and supporting CIS operations are—

- Task organization and command/support relationships of MAGTF CI units—CI/HUMINT Co headquarters collocated with the MAGTF G-2/S-2 CIC/IOC. Although company elements normally operate in GS of the MAGTF, task-organized CI, IT or HSTs may be either attached or placed in direct support of MAGTF subordinate units.
- Principal CI systems (e.g., CHATS) employed within and in support of the MAGTF.
- Communications connectivity—the principal communications pathways and the level of security classification.

5005. CI CIS PLANNING CONSIDERATIONS

The following identifies key CIS requirements and planning considerations supporting MAGTF CI operations.

- Ensure that the MAGTF CE G-2/S-2, intel bn, CI/HUMINT Co elements, and other MAGTF units are included in the distribution of CI/HUMINT-related address indicator groups to receive pertinent JTF, theater, and national intelligence and CI products.
- Determine and coordinate radio net requirements, supporting frequencies, and operational procedures supporting CI operations (external to MAGTF, internal MAGTF, intelligence broadcasts, retransmission sites, routine and time-sensitive operations, etc.).
- Coordinate CI CIS activation and restoration priorities and supporting procedures.
- Determine cryptograph material system requirements for unique CI communications.
- Determine and coordinate wire communications (including telephones) supporting CI operations.
- Establish, operate, and manage unique CI communications.
- Determine and coordinate local and wide area networks and unique intelligence networks information systems requirements in support of CI operations (hardware, software, Internet protocol addresses, etc.).

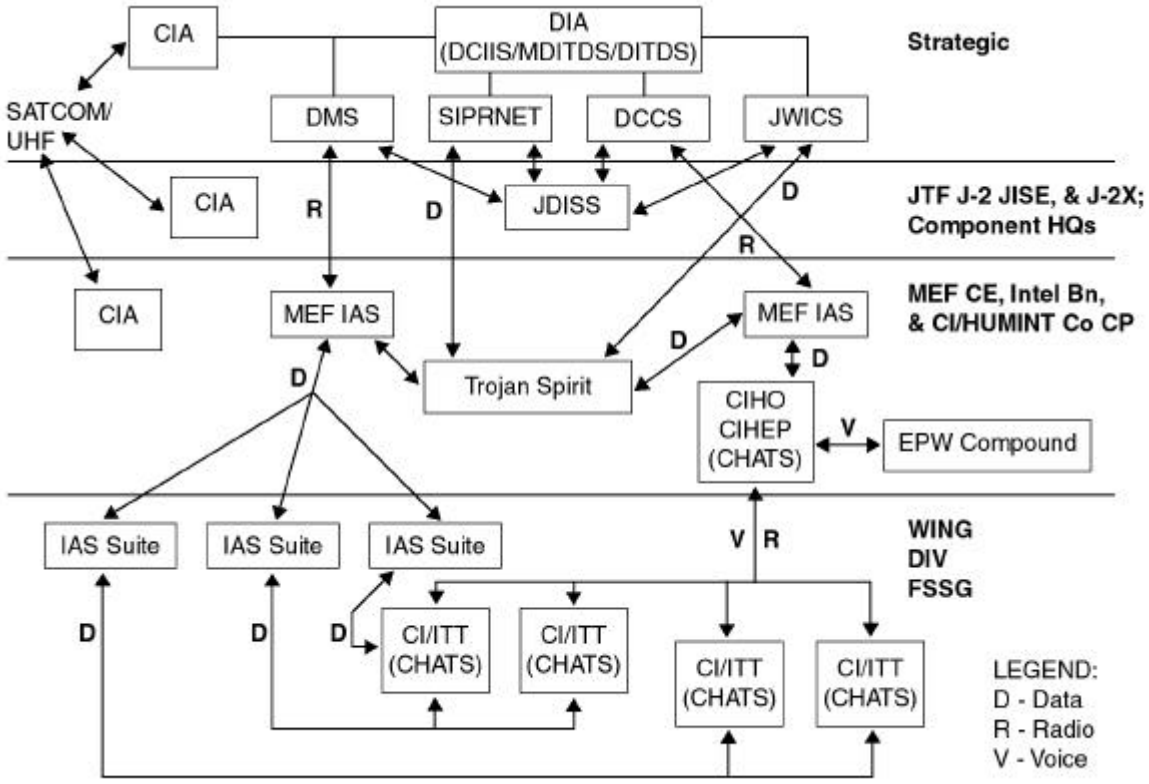

Figure 5-6. Counterintelligence Architecture.

- Integrate CI/HUMINT elements' CIS operations with those of other MAGTF and pertinent JTF and other components intelligence and reconnaissance units (mutual support, cueing, etc.).
- Integrate communications of CI/HUMINT elements employed in GS with collocated GCE, ACE, CSSE, and other MAGTF elements (e.g., to provide time-sensitive reporting, coordination of maneuver, etc.).
- Coordinate CI CIS and dissemination operations and procedures with allied and coalition forces.

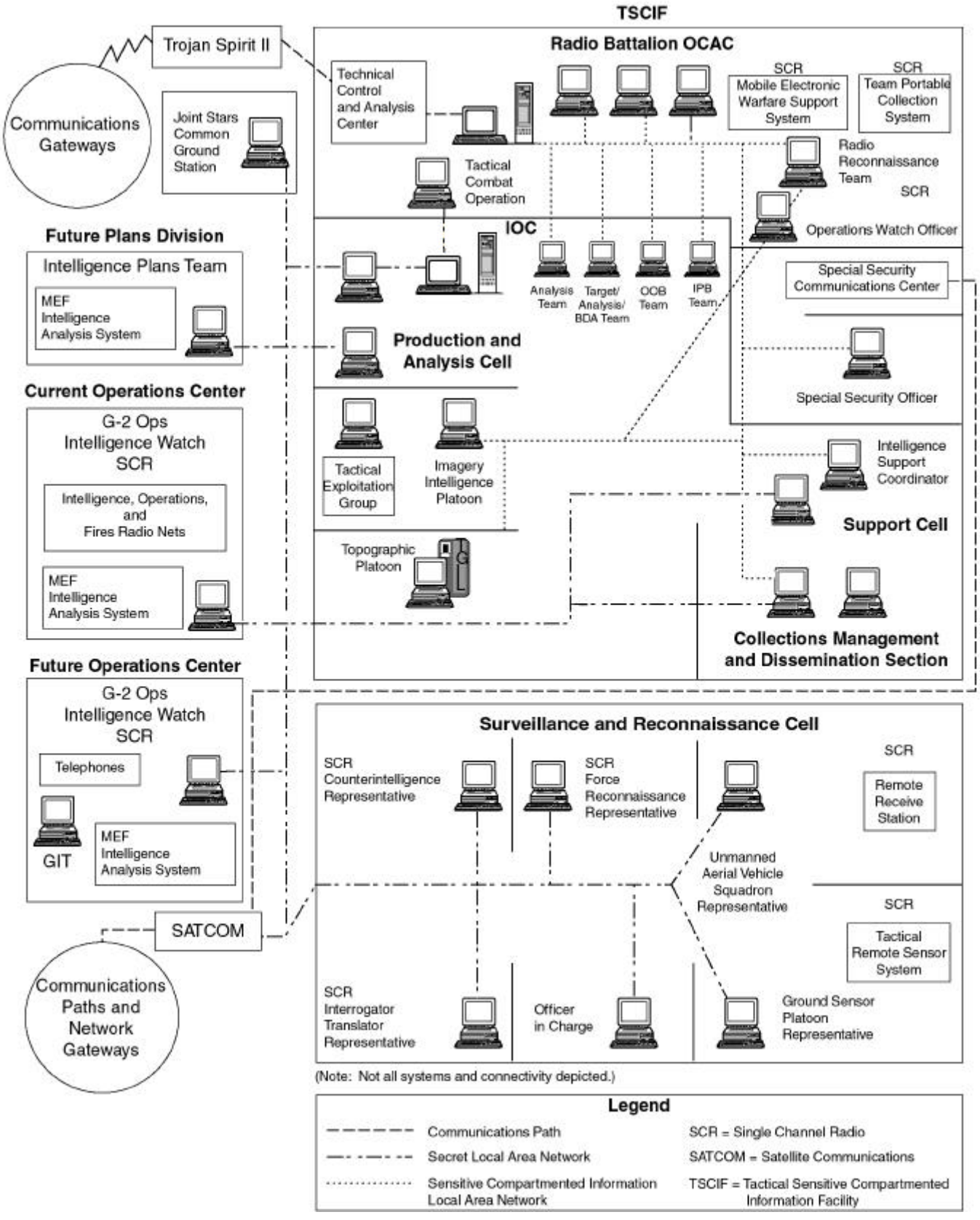

Figure 5-7. CI Elements within the MAGTF CE CIC and IOC and Key Communications and Informations Systems.

CHAPTER 6. COUNTERINTELLIGENCE PLANNING

6001. MARINE CORPS PLANNING PROCESS AND JOINT PLANNING PROCESS OVERVIEW

Planning is an act of preparing for future decisions in an uncertain and time-constrained environment. Whether it is done at the national or the battalion/squadron level, the key functions of planning are—

- Planning leads to a plan that directs and coordinates action.
- Planning develops a shared situational awareness.
- Planning generates expectations about how actions will evolve and affect the desired outcome.
- Planning supports the exercise of initiative.
- Planning shapes the thinking of planners.

Marine Corps Planning Process

The Marine Corps Planning Process (MCPP) helps organize the thought processes of commanders and their staff throughout the planning and execution of military operations. It focuses on the threat and is based on the Marine Corps warfighting philosophy of maneuver warfare. It capitalizes on the principle of unity of effort and supports the establishment and maintenance of tempo. The MCPP steps can be as detailed or as abbreviated as time, staff resources, experience, and the situation permit. It applies to command and staff actions at all echelons. From the Marine Corps component headquarters to the battalion/squadron level, commanders and staff members must master the MCPP to be full participants in integrated planning. Additionally, the MCPP complements deliberate or crisis action planning (CAP) as outlined in the Joint Operation Planning and Execution System (JOPES).

See MCWP 5-1, *Marine Corps Planning Process*, for detailed doctrine and TTP regarding the MCPP. JP 5-00.2, *Joint Task Force Planning, Guidance and Procedures* provides detailed discussion of the joint planning process.

The MCPP (see figure 6-1 on page 6-2) establishes procedures for analyzing a mission, developing and analyzing COAs against the threat, comparing friendly COAs against the commander's criteria and each other, selecting a COA, and preparing an OPORD for execution. The MCPP organizes the planning process into six steps. It provides commanders and their staff a means to organize their planning activities and transmit the plan to subordinates and subordinate commands. Through this process, MAGTF levels of command can begin the planning effort with a common understanding of the mission and commander's guidance.

The six integrated steps of this process are—

- **Mission analysis.** Mission analysis is the first step in planning. The purpose of mission analysis is to review and analyze orders, guidance, and other information provided by higher headquarters and produce a unit mission statement. Mission analysis drives the MCPP.
- **COA development.** During COA development, the planners use the mission statement, including higher headquarters tasking and intent,

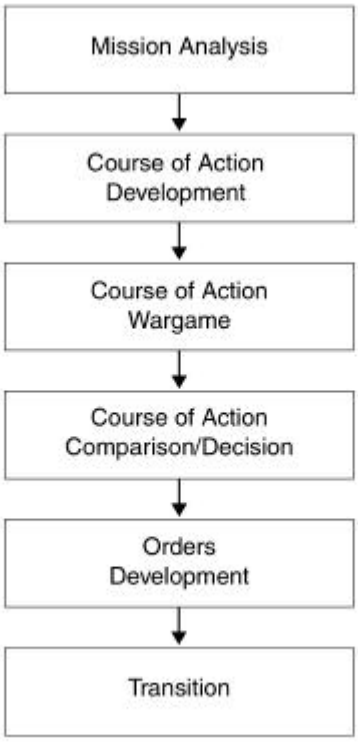

Figure 6-1. The Marine Corps Planning Process.

commander's intent, and commander's planning guidance to develop the COA(s). Each prospective COA is examined to ensure that it is suitable, feasible, distinguishable, acceptable, and complete with respect to the current and anticipated situation, the mission, and the commander's intent. Per the commander's guidance, approved COAs are further developed in greater detail.

- **COA wargaming.** During COA wargaming, each friendly COA is examined against selected threat COAs. COA wargaming involves a detailed assessment of each COA as it pertains to the threat and the environment. It assists the planners in identifying strengths and weaknesses, associated risks, and asset shortfalls for each friendly COA. It identifies branches and potential sequels that may require additional planning. Short of actually executing the COA, COA wargaming provides the most reliable basis for understanding and improving each COA.
- **COA comparison and decision.** In COA comparison and decision, the commander evaluates all friendly COAs—against established criteria, then against each other—and selects the COA that he deems most likely to accomplish the mission.
- **Orders development.** During orders development, the staff takes the commander's COA decision, mission statement, commander's intent, guidance, and develops orders to direct the actions of the unit. Orders serve as the principal means by which the commander's decision, intent, and guidance are expressed.
- **Transition.** Transition is an orderly handover of a plan or order passed to those tasked with execution of the operation. It provides those who will execute the plan or order with the situational awareness and rationale for key decisions necessary to ensure there is a coherent shift from planning to execution.

Comparison of the MCPP and the Joint Planning Processes

Joint Deliberate Planning

The deliberate planning process is used by the joint staff and commanders in chief (CINCs) to develop plans (OPLANs, CONPLANs, functional plans) supporting national strategy. The Joint Strategic Capabilities Plan apportions forces and resources for use during deliberate planning by the combatant commanders and their service component commanders. Figure 6-2 illustrates how the MCPP fits within and supports the joint deliberate planning process.

Interactions among various planning steps allow a concurrent, coordinated effort that maintains flexibility, makes efficient use of time available, and facilitates continuous information sharing.

Crisis Action Planning (CAP)

CAP is conducted in response to crises where national interests are threatened and a military response is being considered. In CAP, the time available for planning at the national level may be as little as a few days. CAP procedures promote the logical, rapid flow of information and the timely preparation of campaign plans or OPORDs. The figure 6-3 on page 6-4 illustrates how the MCPP fits within and supports the joint crisis action planning process.

6002. CI PLANNING

Intelligence Planning

CI planning and execution is conducted in concert with the six phases of the standard intelligence cycle. The first phase is planning and direction. It consists of those activities that identify pertinent intelligence requirements (IR) and provides the means for satisfying those requirements. Intelligence planning and direction is a continuous function and a command responsibility. The commander directs the intelligence effort; the intelligence officer manages this effort for the commander based on the intent, designation of priority intelligence requirements (PIRs) and EEFI, and specific guidance provided during the planning process.

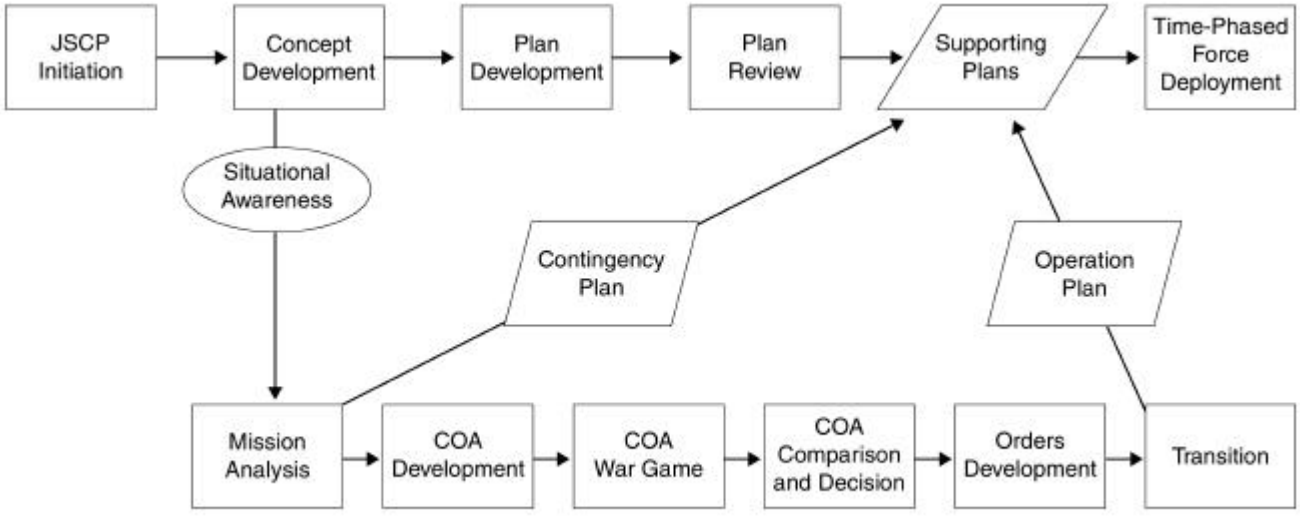

Figure 6-2. The MCPP and the Joint Deliberate Planning Process.

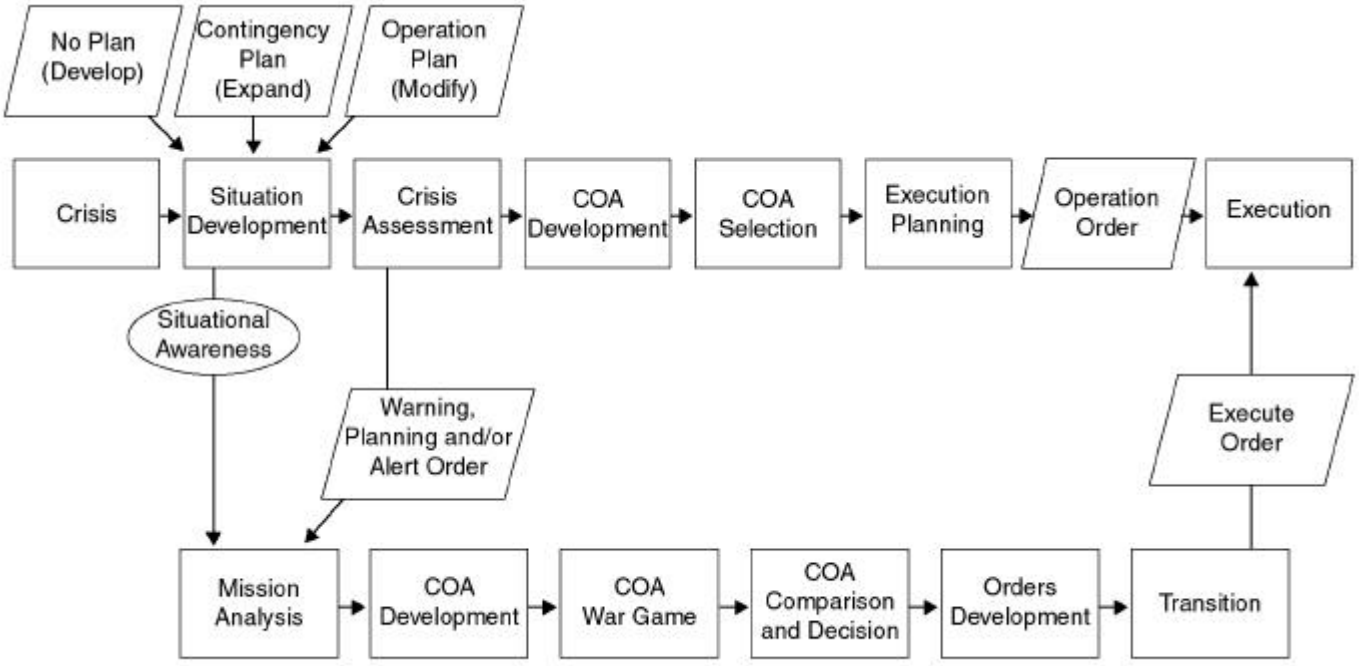

Figure 6-3. The MCPP and the Joint Crisis Action Planning Process.

CI Planning—General

Focus

CI planning and subsequent operations are conducted in support of the MAGTF or designated subordinate commanders to support the overall intelligence effort and to aid with force protection. Accordingly, CI must be planned with the overall intelligence and force protection efforts. The commander must incorporate CI early in the planning process to formulate an estimate of the situation, identify the MAGTF's risks and security vulnerabilities, and begin shaping overall and supporting intelligence and force protection operations.

Planning and Direction Functions

- Requirements development.
- Requirements management.
- Collection management.
- Production management.
- Dissemination management.

CI and HUMINT

CI must be considered with many other intelligence activities because of the mission of CI. HUMINT is the intelligence activity that has the most important connective tie to CI. CI and HUMINT work hand-in-hand because of the nature of their targets and the type of intelligence missions they perform: CI neutralizing the enemy intelligence effort and HUMINT collecting information about enemy activity. The differentiation and coordination required for the effective exploitation of human sources is critical, requiring integration of CI activities and HUMINT operations (e.g., IT exploitation of EPW). See DIAM 58-11, *DOD HUMINT Policies and Procedures*, and DIAM 58-12, *The DOD HUMINT Management System*, for additional information.

See chapter 3 of MCWP 2-1 for comprehensive discussion of each phase of the intelligence cycle, intelligence requirements management, and the overall conduct of intelligence planning and direction.

CI Planning Responsibilities

See paragraphs 3002 and 3003.

Coordination Considerations

The complexity of CI operations requires thorough coordination with intelligence organizations. Detailed coordination ensures that CI operations are focused on intelligence priorities and are not duplicative. Constant coordination must be accomplished with the JTF and other component forces, combatant commander, and other supporting intelligence organizations to ensure coordinated, manageable, and effective CI operations are conducted.

CI Planning Considerations

Key considerations in planning CI operations include—

Friendly Considerations. CI operations must support and adapt to the commander's intent, concepts of intelligence and operations, and the supporting scheme of maneuver. Questions to answer include—

- What are the MAGTF areas of operations (AO) and areas of interest (AI)?
- What are the MAGTF concept of operations, task organization, main and supporting efforts?
- What are the task organization and the C2 command/support relationships among MAGTF intelligence, CI and reconnaissance units? Can the friendly concept of operations be supported by CI elements operating in MAGTF GS, or are CI direct support/attachments to MAGTF subordinate units required? What are the standing PIRs and IRs? Which have been tasked to supporting CI units? What specific information is the commander most interested in (i.e., enemy air operations, enemy ground operations, friendly force protection, target BDA, or enemy future intentions)?
- What is the MAGTF force protection concept of operations? What are the standing EEFIs and their assessed priorities?
- What are the CI, intelligence and force protection concepts of operations of the JTF, other components and theater forces? How can external CI assets be best integrated and employed to support MAGTF operations?

Enemy Considerations

Intelligence operations focus on the enemy. Prior to commencing MAGTF CI operations, we must learn as much as we can about the enemy. Key adversary information which must be considered when conducting CI planning include—

- What threat forces—conventional, law enforcement/security, paramilitary, guerrilla, terrorist—are within the MAGTF AO and AI? What are their centers of gravity and critical vulnerabilities? Is this a large enemy force organized along conventional military lines or a small, loosely knit guerrilla or unconventional military force? What are their sizes, composition, tactics, techniques, and procedures?
- Who are the key enemy military, security, and civilian leaders? What and where are the enemy's critical nodes for C2 and what are their vulnerabilities? What security countermeasures do they employ to prevent CI exploitation of their operations? What are its C2 and CIS tactics, techniques, and procedures?

- Who are the known enemy personalities engaged in intelligence, CI, security, police, terrorist, or political activities? Who are known or suspected collaborators and sympathizers, both within the populace and within other parties?
- What are the key installations and facilities used by enemy intelligence, espionage, sabotage, subversive, and police organizations? What are the key communications, media, chemical, biological, utilities, and political installations and facilities?
- What are the national and local political parties or other groups known to have aims, beliefs, or ideologies contrary or in opposition to those of the U.S.? What are the student, police, military veterans, and similar groups known to be hostile to the U.S.?

6003. CI PLANNING AND THE INTELLIGENCE CYCLE

General

The intelligence cycle is a procedural framework for the development of mission-focused intelligence support. It is not an end in itself, nor should it be viewed as a rigid set of procedures that must be carried out in an identical manner on all occasions. The commander and the intelligence officer must consider each IR individually and apply the intelligence cycle in a manner that develops the required intelligence in the most effective way.

The application of the intelligence cycle will vary with the phase of the planning cycle. In theory, a unique iteration of the intelligence cycle is carried out for each individual requirement. In practice, particularly during the planning phase, requirements are grouped together and satisfied through a single, concurrent intelligence development process that addresses CI requirements. During the planning phase, intelligence development is generally carried out through two major iterations of the intelligence cycle. The first primarily supports decision planning. Completion of this iteration of the intelligence cycle results in the preparation and use of basic intelligence and CI products-intelligence and CI estimates, supporting studies, and IPB analysis-that describe the battlespace and threat. These products form the basis for development and selection of MAGTF COAs. The second iteration of the intelligence cycle supports execution planning. It is an outgrowth of the selection of the COA and formulation of the concept of operations; the implementation of the intelligence collection, production and dissemination plan; refinement of IPB analysis, and the generation of mission-specific intelligence products and CI measures integrated with the concept of operations to support mission execution. During execution, requirements are satisfied on a more individualized basis. New requirements are usually generated in response to a specific operational need. Each requirement is unique and must be satisfied in a timely manner to facilitate rapid decisionmaking and the generation or maintenance of tempo (see figure 6-4).

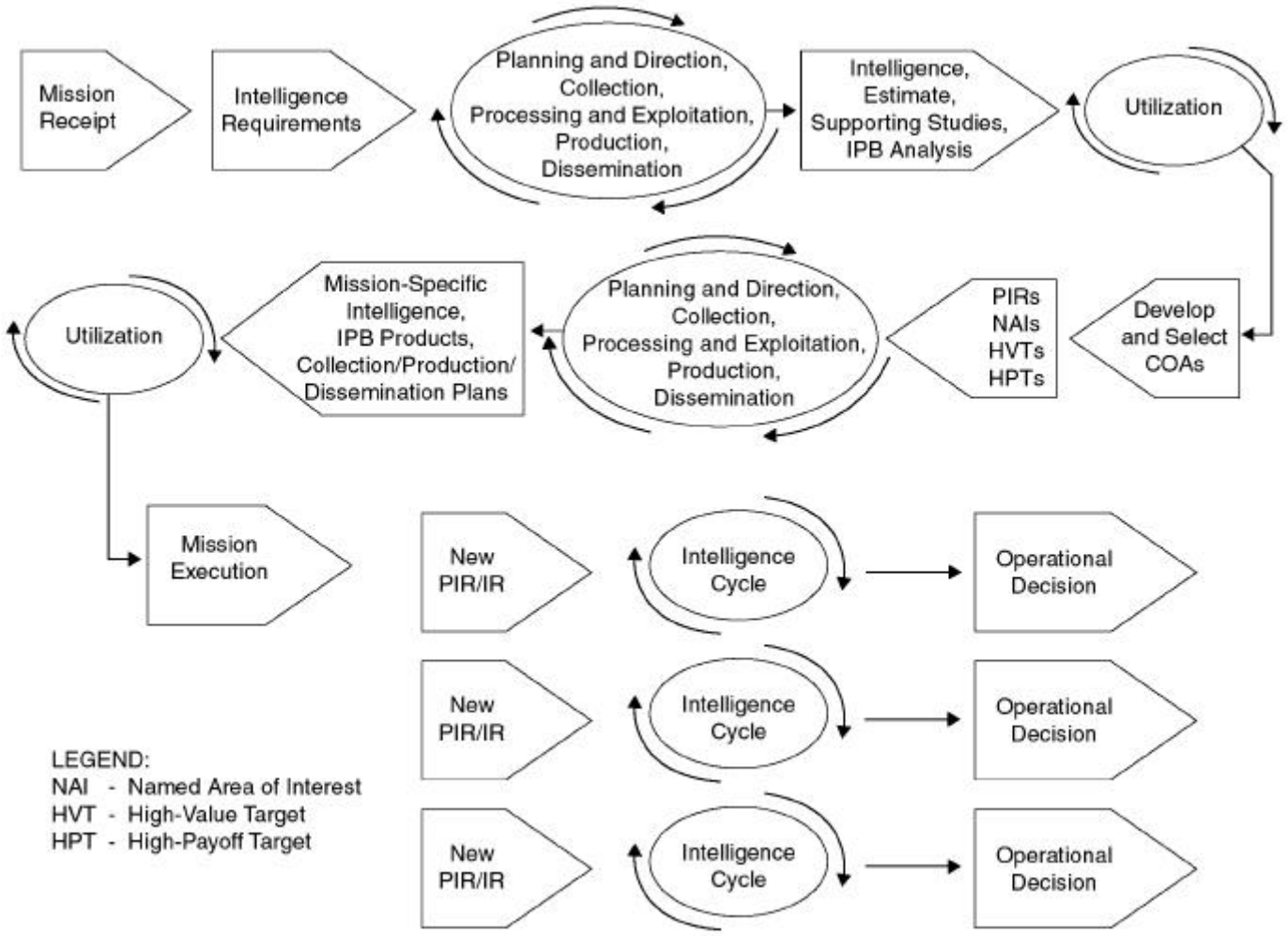

Figure 6-4. Application of the Intelligence Cycle.

The G-2/S-2 provides CI participation and assistance early in the planning phase of tactical operations. Commanders benefit from CI information given at this phase because it helps to formulate tactical plans and because CI/ HUMINT operations generally require more time than other intelligence disciplines to yield substantive results. CI also provides the commander with capabilities that are offered by no other discipline or technical system. CI is one of the tools that can help the commander anticipate the action of the enemy. Particular attention is directed to identifying friendly vulnerabilities to be exploited by hostile collection assets and to recommending specific CI measures.

The CI effort focuses on the overall hostile intelligence collection, sabotage, terrorist, and subversive threat. The CI effort is also sufficiently flexible to adapt to the geographical environment, attitudes of the indigenous population, mission of the supported command, and changing emphasis by hostile intelligence, sabotage, terrorist, and subversive organizations.

Planning the Activity

The effectiveness of MAGTF CI operations depends largely on the planning preceding the operation. The G-2/S-2 performs four separate functions in

carrying out CI planning responsibilities. First, the effort is directed to collect information on the enemy's intelligence, sabotage, terrorism, and subversion capabilities, coordinating with the ISC, CMDO, and CI/HUMINT Co commander, ensuring CI collection requirements levied upon CI/HUMINT elements are realistic and within the capability of the CI elements and are integrated into the MAGTF's all-source intelligence collection plan. Second, with the ISC, the P&A cell OIC, and the G-3/S-3 force protection planners, the G-2/S-2 supports the production of intelligence on the enemy's intelligence, sabotage, terrorism, and subversion capabilities, including clandestine and covert capabilities. Third, with the ISC and the CMDO, timely dissemination of CI products are assured to MAGTF units. Finally, the G-2/S-2 plans, recommends, and monitors CI measures throughout the command.

CI Collection and Processing of Information

CI elements can collect both CI and intelligence information through the use of overt tactical source HUMINT operations. The determination of CI collection requirements follows the same process and procedures prescribed for other types of IRs (see MCWP 2-1, chapter 3). Especially pertinent to CI planning is information on the enemy's intelligence and reconnaissance capabilities and operations. Included are such matters as the hostile intelligence organization, means available to the enemy for the collection of information, and hostile sabotage, terrorism, and subversive agencies and capabilities.

The area commander normally provides the procedures and authority governing the conduct of overt tactical source HUMINT and certain offensive CI operations. These procedures are covered in detail in the classified addendum, DIAM 58-11, DIAM, and theater collection plans.

CI Collection Sources. CI sources of information include—

- **Casual Sources.** A casual source, by social or professional position, has access to information of CI interest, usually on a continuing basis. Casual sources usually can be relied on to provide information routinely available to them. They are under no obligation to provide information. Casual sources include private citizens, such as retired officials or other prominent residents of an area. Members of private organizations also may furnish information of value.
- **Official Sources.** Official sources are liaison contacts. CI personnel conduct liaison with foreign and domestic CI intelligence, security, and law enforcement agencies to exchange information and obtain assistance. CI personnel are interested in investigative, operational, and threat information.
- **Recruited Sources.** Recruited sources include those who support CFSO and are by design, human source networks dispersed throughout the AO who can provide timely and pertinent force protection information.
- **Refugees, Civilian Detainees, and EPWs.** Refugees, civilian detainees, and EPWs are other sources of CI information. The key to identifying the source of valuable CI force protection information is in analyzing the information being sought and predicting who, by virtue of their regular duties, would have regular, frequent, and unquestioned access to such information.
- **Open Sources.** Open source publications of all sorts (newspapers, magazines, etc.) and radio and television broadcasts are valuable sources of information of CI interest and information. When information is presented in a foreign language, linguist support is required for timely

translation. Depending on the resources, this support can be provided by MAGTF IT personnel, allied personnel, or indigenous employees.

- **Documents.** Documents not openly available, such as adversary plans and reports, are exploited in much the same way as open source publications.

CI Targets. CI targets include personalities, organizations, and installations (PO&I) of intelligence or CI interest, which must be seized, exploited, neutralized or protected. The PO&I targeting triad forms the basis of CI activities. Incidents are also included within CI data bases to conduct trend analysis of potential targets. DIA has the responsibility, in response to a validated requirement, to establish and maintain CI data bases. Operational control of the data base will pass to the JTF HQ, once deployed.

The P&A cell's CI analytical team has the responsibility of establishing and maintaining CI data bases for the MEF and will coordinate with the local collection elements to eliminate duplication of effort and maximize information sharing (within smaller MAGTFs, the CI/HUMINT Co detachment or HST performs this function).

Selecting and assigning targets is based on an assessment of the overall hostile threat, unit mission, commander's intent, designated PIRs and other IRs, and the overarching intelligence and force protection concepts of operations. The assessment considers both the immediate and estimated future threats to security. It normally is conducted at the MAGTF level where the resultant CI target lists are also produced and include any CI targets assigned by higher headquarters. Numerical priority designations are assigned to each target to emphasize the relative importance and value of the target. Designations also indicate the degree of security threat and urgency in neutralizing or exploiting the target. Priority designations established by higher headquarters are not altered; however, lower echelons may assign priorities to locally developed targets.

CI targets are usually assigned priority designations according to the following criteria:

- **Priority One.** Priority One targets represent the greatest security threat to the MAGTF. They also possess the largest potential source of intelligence or CI information/material that must be exploited or neutralized as soon as possible.
- **Priority Two.** Priority Two targets are of lesser significance than priority one targets. They are to be taken under control after priority one targets have been neutralized or exploited.
- **Priority Three.** Priority Three targets are of lesser significance than priority one or two targets. They are to be neutralized or exploited as time and personnel permit.

Personalities. Except for well-known personalities, most persons of CI interest are identified and developed by CI units once operations have commenced. Personalities are divided into three, color-coded categories: threat to security, intentions unknown, and assist the intelligence and CI effort.

- **DETAIN (Black) List.** A CI listing of actual or potential enemy collaborators, sympathizers, intelligence suspects, and other persons whose presence menaces the security of friendly forces (JP 1-02). The black list includes the following persons:

- Known or suspected enemy or hostile espionage, sabotage, terrorist, political, and subversive individuals.
- Known or suspected leaders and members of hostile paramilitary, partisan, or guerrilla groups.
- Political leaders known or suspected to be hostile to the military and political objectives of the United States and/or an allied nation.
- Known or suspected officials of enemy governments whose presence in the theater of operations poses a security threat to the U.S. Forces.
- Known or suspected enemy collaborators and sympathizers whose presence in the theater of operations poses a security threat to the U.S. Forces.
- Known enemy military or civilian personnel who have engaged in intelligence, CI, security, police, or political indoctrination activities among troops or civilians.
- Other enemy personalities such as local political personalities, police chiefs, and heads of significant municipal and/or national departments or agencies.

Gray lists, compiled or developed at all echelons of command, contain the identities and locations of those personalities whose inclinations and attitudes toward the political and military objectives of the U.S. are unknown.

- **OF INTEREST (Gray) List.** Regardless of their leanings, personalities may be on gray lists when known to possess information or particular skills required by friendly forces. They may be individuals whose political motivations require further exploration before they can be used effectively. Examples of individuals who may be included in this category are:
  - Potential or actual defectors from the hostile cause whose credibility has not been established.
  - Individuals who have resisted, or are believed to have resisted the enemy government and who may be willing to cooperate with friendly forces, but whose credibility has not been established.
  - Nuclear, biological, chemical and other scientists and technicians suspected of having been engaged in enemy weapons of mass destruction and other programs against their will.

- **PROTECT (White) Lists.** White lists, compiled or developed at all echelons of command, contain the identities and locations of individuals in enemy controlled areas. These individuals are of intelligence or CI interest. They are expected to be able to provide information or assistance in the accumulation of intelligence data or in the exploitation of existing or new intelligence areas of interest. They are usually in accord with or favorably inclined toward U.S. policies. Their contributions are based on a voluntary and cooperative attitude. Decisions to place individuals on the white list may be affected by the combat situation, critical need for specialists in scientific fields, and such intelligence needs as indicated from time to time. Examples of individuals included in this category are:
  - Deposed political leaders of a hostile state.
  - Intelligence agents employed by U.S. or allied intelligence agencies.
  - Key civilians in areas of scientific research, including faculty members of universities and staffs of industrial or national research facilities whose credibility have been established.

- Leaders of religious groups and other humanitarian groups.
- Other persons who can significantly aid the political, scientific, and military objectives of the U.S. and whose credibility has been established.

Organizations. These include any organization or group that is an actual or potential threat to the security of JTF or allied forces and must be neutralized. However, an organization or group may present a threat that is not immediately apparent. The enemy frequently camouflages his espionage or subversive activities by establishing front organizations or groups. If these organizations are permitted to continue their activities, they could impede the success of the military operations. Examples of hostile organizations and groups of major concern to the CI unit during tactical operations include—

- Hostile intelligence, sabotage, subversive, and insurgent organizations or groups.
- National and local political groups and parties known or suspected to have aims, beliefs, or ideologies contrary or in opposition to those of the United States.
- Paramilitary organizations, including student, police, military/veterans, and ex-combatant groups, known to be hostile to the U.S.
- Hostile sponsored groups and organizations whose objectives are to create dissension and spread unrest among the civilian population in the AO.

Installations. These include any installation, building, office, or field position that may contain information or material of CI interest or that may pose a threat to MAGTF security. Examples of installation type targets are—

- Installations formerly or currently occupied by enemy espionage, sabotage, subversive, or police organizations, including prisons and detention centers.
- Installations occupied by enemy intelligence, CI, security, or paramilitary organizations, including operational bases, schools, and training sites.
- Enemy communication media and signal communication centers.
- Research centers and chemicals laboratories used in the development of weapons of mass destruction.
- Enemy political administrative headquarters.
- Production facilities, supply areas, and other installations to be taken under control to deny support to hostile guerrilla and partisan elements.
- Public utilities and other installations to be taken under early control to prevent sabotage. These installations are usually necessary for the rehabilitation of civil areas under U.S. control.
- Embassies and consulates of hostile governments.

Incidents. The recording of details of incidents occurring within the AO allows for trend analysis that may reveal patterns and indications of future intentions. Incidents do not occur in a vacuum. They are planned, organized, and carried out by individuals acting alone or in groups. Detailed recording of incidents that occur within an AO is a critical ingredient in the analysis of trends and patterns designed to identify indications of future intentions.

Matrix manipulation, link analysis, and visual investigative analysis are tools often used in the incident analysis process. The matrix allows for a considerable amount of information to be stored in a relatively small space. Link analysis then analyzes these bits of information by displaying the links that exist between them. Visual investigative analysis is used to time sequence names and events to show a clearer picture of these relationships.

CI Target Reduction. The timely seizure and exploitation of CI targets requires a detailed and well-coordinated CI reduction plan. This plan should be prepared well in advance and kept current. CI elements supporting tactical assault units normally prepare the reduction plan. Assigned or developed targets located within the unit's AO, are listed in the reduction plan. This plan is based on the MAGTF's scheme of maneuver, with CI targets listed in the sequence in which they are expected to appear in the AO. However, the target priority designations remain as assigned on the CI target list with highest priority targets covered first when more than one target is located in the same general area. Neutralized and exploited targets are deleted from the CI reduction plan and appropriate reports are submitted. A well-prepared and comprehensive CI reduction plan ensures coverage of significant CI targets. It also allows CI units to conduct daily operations based on established priorities. (See appendix D for a sample CI reduction plan.)

CI Measures Worksheet. The CI worksheet is prepared or revised based on the conclusions reached in the intelligence estimate of the enemy capabilities for intelligence, subversion, terrorist activities, and sabotage. This worksheet is an essential aid in CI planning. It is also the basis for preparing CI orders and requests. (See appendix D for a sample CI measures worksheet.)

CI Analysis and Production

Offensive

- Targeting for fire and maneuver.
- Physical security.
- Counterreconnaissance.
- Countersabotage.
- Penetration and exploitation operations.

Defensive

- Deception operations (OPSEC).
- Counterespionage operations.
- Information security.
- Personnel security. Counterterrorism

Analysis and production is the heart of CI despite the quality and quantity of information is gathered, it will be worthless if is not turned into intelligence and disseminated to commanders and planners in time to use for decisionmaking. Critical to the success of MAGTF CI activities is taking collected information and producing tactically relevant intelligence (usually via all-source intelligence production), and providing it to commanders and planners in a timely manner. The transition of raw information into finished intelligence is the process of analysis. Fusing the finished intelligence into something usable by the customer is known as production.

CI Production Threat Focus. CI analysis and production is focused on three well-defined threat activities: HUMINT, IMINT, and SIGINT.

- **Counter Human Intelligence (C-HUMINT).** C-HUMINT requires effective and aggressive offensive and defensive measures. Our enemies collect against MAGTFs using both sophisticated and unsophisticated methods. We must combat all of these methods to protect our force and to ensure the success of our operations. MAGTF CI elements recommend countermeasures developed by CI analysts that the commander can take against enemy collection activities. CI C-HUMINT analysis focuses not only upon the standard enemy CI targets within the AO, but also upon the intelligence product most likely being developed through their collection

activities. The analytical effort should attempt to identify the enemy's HUMINT cycle (collection, analysis, production, targeting) and key personalities. To produce a complete and accurate analysis and then develop effective products, CI analysts may need access to considerable data and require significant resources. CI analysts will require collection in the areas of subversion, espionage, sabotage, terrorism, and other HUMINT supported activities. Collection of friendly force data is also required to substantiate CI analytical findings and recommendations. Consistent with time, mission, and availability of resources, efforts must be made to provide an analytical product identifying the enemy's intelligence, espionage, subversion, sabotage, and terrorism efforts. To accomplish C-HUMINT, MAGTF CI elements will conduct CI investigations, collections, and operations. Key C-HUMINT tasks include—

- Identifying the hostile HUMINT collectors and producers.
- Developing, maintaining, and disseminating multi-discipline threat data and intelligence on organizations, locations, and individuals of CI interest. This includes insurgent and terrorist infrastructure and individuals assisting in the CI mission. It also includes performing personnel security investigations and records checks on persons in sensitive positions and whose loyalty is questionable. Also, personnel must be educated and trained in all aspects of command security. A component of this is the multi-discipline threat briefing. Briefings can and should be tailored, both in scope and classification level. Briefings can then be used to familiarize MAGTF units with the nature of the multi-discipline threat posed against the command or activity. Additionally, CI elements must search for enemy personnel who pose an intelligence collection or terrorist threat to the MAGTF. Should CI investigations result in identifying the location of terrorists, their apprehension is done with military, civil, and law enforcement authorities. Also, debriefing of selected personnel (friendly and hostile) including combat patrols, aircraft pilots, or other elements possessing information of CI interest is necessary.

See appendix C, section I, for additional information on C-HUMINT.

- Neutralizing or exploiting these to deny the enemy key friendly force information.
- Controlling our own information and indicators of operations so they are not readily accessible to the enemy's HUMINT operations.
- Supporting C-HUMINT commanders through effective and stringent adherence to physical, information, and personnel security procedures. They apply force or assets to ensure security daily. MAGTF CI and intelligence elements provide continuous and current threat information so the command can carry out its security responsibilities.

- **Counter Imagery Intelligence (C-IMINT).** C-IMINT requires CI analysts to have an in-depth knowledge of the supported commander's plans, intentions, and proposed AO as far in advance as possible. CI analysts must have access to available data and intelligence on enemy IMINT methodology, systems, and processing as well as in-depth information on commercial satellite systems and the availability of their products to the enemy or to other supporting parties. CI analysts attempt to define the specific imagery platform deployed against the MAGTF and the cycle involved (time-based) from time of imaging through analysis to targeting. Knowledge of enemy intelligence support to targeting is critical in developing countermeasures to defeat, destroy, or deceive enemy IMINT. For ground-based HUMINT oriented IMINT (video cassette

recorders, cameras, host nation curiosity, news media organizations), MAGTF CI elements will be required to collect the data for analysts. This type of information cannot be reasonably considered to exist in any current data base. Traditional enemy IMINT data is readily available and should not require any CI collection effort. However, collection to support CI (overflights of friendly forces by friendly forces) during identified, critical, and IMINT vulnerable times will validate CI C-IMINT findings and support countermeasures planning and execution. This will be of immense value to the CI analyst and the supported commander in determining what enemy imagery has been able to exploit. (See appendix C, section II, for additional information on C-IMINT.) The enemy may possess or acquire IMINT systems or products with comprehensive and sophisticated capabilities. The MAGTF must have in place carefully developed countermeasures to negate any tactical and strategic threat. The enemy may acquire IMINT through a variety of ways, from handheld cameras to sophisticated satellite reconnaissance systems. Such IMINT capabilities may include—

- Aerial cameras.
- Infrared sensors.
- Imaging radars.
- Electro-optical sensors (TV).
- Multispectral and digital imagery products.

Offensive

- Targeting for fire and maneuver.
- Electronic attack.

Defensive

- OPSEC countermeasures.
- Use of secure telephone.
- Signals security procedures.
- Deception operations.

- **Counter Signals Intelligence (C-SIGINT).** C-SIGINT operations, including COMSEC monitoring and information systems security, are conducted during peace, war, and MOOTW to enhance MAGTF force protection, survivability, mobility and training; provide data to identify friendly CIS vulnerabilities; develop countermeasures recommendations and plans; and when implemented, determine if countermeasures are effective. C-SIGINT includes full identification of the threat and an integrated set of offensive and defensive actions designed to counter the threat. Counter-SIGINT focuses upon the enemy's entities that can conduct SIGINT and EW against friendly forces. It also focuses on the intelligence that is most likely being collected and produced from their efforts. C-SIGINT analysis effort should be fully automated (data storage, sorting, and filing). CI analysts require SIGINT data collection to support vulnerability assessment and countermeasure evaluation. Validation of vulnerabilities (data and operations that are exploitable by the enemy's SIGINT operations) and the effectiveness of implemented countermeasures (a before and after comparison of MAGTF electromagnetic signatures and data) will be nearly impossible without active and timely collection as a prerequisite to analysis. CI analysts require a comprehensive data base consisting of enemy SIGINT systems, installations, methodology, and associated SIGINT cycle information. Friendly CIS systems and user unit identification must be readily available, as well as a library of friendly countermeasures and a history of those previously implemented countermeasures and results achieved. CI analysts should, at any given time, be able to forecast enemy SIGINT activity. However, such estimates must rely upon other CI, SIGINT, and IMINT collection and access to adjacent friendly unit CI files. Information on enemy SIGINT must be readily accessible from intelligence elements higher as well as lower in echelon than the supported command. Effective conduct of C-SIGINT requires close coordination and integrated production between MAGTF CI, SIGINT and

all-source intelligence producers. C-SIGINT provides commanders and planners with the knowledge to assess the risk and probable success of alternative courses of action before a plan is implemented. C-SIGINT is a cyclic process requiring a strong analytical approach integrating MAGTF CI, SIGINT, CIS and force protection personnel. C-SIGINT is based on a thorough knowledge of—

- Enemy SIGINT capabilities and tactics, techniques and procedures.
- MAGTF and other friendly forces' communications and information systems profile.
- Enemy operations and plans.
- Realistic security measures, both INFOSEC and physical, that can be taken to deny information to the enemy. (See appendix C, section III, for additional information on C-SIGINT.)

CI Analytical and Production Functions. CI analysts perform the following analytical and production functions:

- Analyze the multi-discipline intelligence, espionage, subversion, sabotage, and terrorism threats targeted against the MAGTF.
- Assess enemy intelligence vulnerabilities and susceptibilities to friendly deception efforts and other countermeasures.
- Support MAGTF force protection vulnerability assessment.
- Develop, evaluate, and recommend countermeasures to reduce, eliminate, or take advantage of MAGTF vulnerabilities.
- Support rear area operations by identifying intelligence, espionage, subversion, sabotage and terrorism threats to rear area units and installations (to include low-level agents responsible for sabotage and subversion).
- Nominate CI targets for exploitation, neutralization, or destruction.
- Develop and maintain a comprehensive and current CI data base.
- Identify CI IRs and provide these to the collection officer.

CI Products. CI products convey pertinent intelligence resulting from CI analysis to the commanders and planners in a readily useable form. CI analysts prepare a range of products; some focused upon specific needs and others of a more general nature. Among these products of most use to commanders and planners are CI estimates, surveys/vulnerability assessments, summaries, and threat assessments.

- **CI Estimate.** Within the MAGTF a CI estimate is normally prepared only by the ISC for the MAGTF G-2/S-2 and disseminated throughout the MAGTF. The CI estimate forms the basis of the CI plan and operations. It includes the enemy's capabilities and limitations for intelligence, subversion, terrorism, sabotage, and the effects of the characteristics of the area on these capabilities and friendly CI measures. If a CI estimate is not prepared, such CI planning information can be consolidated within the basic intelligence estimate (appendix 11 to annex B, Intelligence). Key parts of the CI estimate include sections on enemy intelligence, subversion, sabotage, guerrilla warfare, terrorism, and the effects of the area on these enemy capabilities. See appendix C for a sample format of a MAGTF CI estimate.
- **CI Survey/Vulnerability Assessment.** CI surveys/vulnerability assessments are studies conducted to provide a supported command or

agency a picture of its susceptibility to foreign intelligence collection. The CI survey/vulnerability assessment assesses a unit's security posture against threats detailed in the CI estimate. The survey should identify vulnerabilities to specific hostile intelligence, espionage, sabotage, subversion or terrorist capabilities and provide viable recommendations to eliminate or minimize these vulnerabilities. The survey should be as detailed as possible. It will usually be prepared by the CI/HUMINT Co, drawing on the expertise of other disciplines such as engineers, military police, civil affairs, and other intelligence and reconnaissance personnel. The survey must look forward, in both space and time, to support the development of CI measures necessary to protect the unit as it carries out successive phases of the operation. The objective of a CI survey/ vulnerability assessment provides commanders a realistic tool to evaluate internal force protection or security programs, and to provide a decisionmaking aid for the enhancement of these programs. CI surveys/ vulnerability assessments include—

- Estimating the enemy's likely PIRs and then evaluating the enemy's and any potential supporting forces' multi-discipline intelligence collection and production capabilities to answer these. Identifying MAGTF and other friendly forces' activity patterns (physical and electronic), friendly physical and electronic signatures, and resulting profiles to enhance OPSEC.
- Monitoring or collecting MAGTF and other friendly forces' CIS transmissions to aid in vulnerability assessments, and providing a more realistic and stable basis to recommend countermeasures. (Note: these operations are generally conducted either by elements of the radio battalion or other supporting elements.)
- Identifying MAGTF and other friendly forces' vulnerabilities based upon analysis of collected information and recommendations of countermeasures.
- Analyzing the effectiveness of implemented countermeasures. See appendix D for a CI survey checklist and the format for a CI survey/vulnerability assessment.

- **Counterintelligence Summary (CISUM).** CISUM is a graphic portrayal of the current situation from a CI point of view. It will be prepared either by the P&A cell or the CI/HUMINT Co's operations/analysis element. CI analysts use the CISUM to show known adversary intelligence units as well as known/estimated threats within the friendly area. CISUM is a periodic report usually covering a 12-hour period. It shows friendly targets identified as adversary objectives during the specified timeframe. CI analysts include a clear, concise legend on each CISUM showing the time period, map reference, and symbols identifying friendly and adversary information. As analysts identify a friendly critical node, element, or resource as an adversary combat or intelligence collection target, they put a box around it and label it with a T number. The legend explains whether the T is—
  - An enemy intelligence target.
  - A source and time confirmation.
  - An enemy resource or element that will attack or collect against the target in the future.
  - The expected timeframe for the enemy to exploit the target.
  - The CISUM might portray the following information:
  - Satellite or tactical reconnaissance patterns over the AO.

- Sweeps by enemy side looking airborne radar (SLAR) or EA air platforms to the full extent of their maximum ranges.
- Suspected landing zones or drop zones that will be used by an enemy element in the rear area.
- Area or unit that has received unusual enemy jamming or other electronic attacks. Movement of an enemy mobile SIGINT site forward along with a graphic description of the direction and depth of its targeting.
- Location of an operational enemy agent or sabotage net.
- Last known location of threat special operations forces.

- **CI Threat Assessment.** The CI threat assessment (see page 6-18) is a four-paragraph statement which is published as often as necessary or when significant changes occur, depending on the situation and the needs of the commander. The CI threat assessment provides justification for CI target nominations and guidance for CI production. It will generally be produced through a combined effort of the P&A cell and the CI/HUMINT Co's operations/analysis element. Essentially, the CI threat assessment provides the following:
  - A quick overview of significant activity during the reporting period.
  - An assessment of the intelligence damage achieved by the enemy.
  - A projected assessment of enemy activity for the next reporting period.
  - CI target nominations.

CI Dissemination

Refer to chapter 5 for a detailed review of CI dissemination planning considerations.

6004. CI PLANNING REQUIREMENTS AND CONSIDERATIONS

The following describes the CI planning requirements, considerations, and activities. It is provided as a guide for MAGTF intelligence, force protection, and CI personnel in planning MAGTF operations.

Formulation of the Commander's Estimate

CI planning activities follow a logical sequence consistent with the MCPP and the six functions of intelligence.

- Provide assistance to the command operations security program. During the initial planning phase, CI assets provide assistance to the G-3/S-3 in establishing force protection planning and operations.
- Complete studies of the enemy organization, weapons and equipment, techniques, and effectiveness in conducting intelligence, subversion, terrorism, and sabotage operations. Timely completion and dissemination throughout the MAGTF of the CI estimate is critical.
- Complete the CI survey/vulnerability assessment to assist with MAGTF force protection planning and countermeasures development and implementation.
- Release CI planning information and products per PIRs and IRs and specified reporting criteria established by the CMDO or as directed by the G-2/S-2. It is critical that CI personnel follow-up with recipients of these products to ensure information is understood and to identify early any resulting new CI IRs.

COUNTERINTELLIGENCE THREAT ASSESSMENT

1. (U) Enemy Activity During Period___ to ___

   a. (U) HUMINT: Summarize in one paragraph all know HUMINT activity during the reporting period. Compile data from HUMINT situation overlay, matrices, link diagrams, and other CI products.

   b. (U) SIGINT: Summarize in one paragraph all known SIGINT activity. Compile from SIGINT situation overlay, matrices, and other CI products.

   c. (U) IMINT: Summarize in one paragraph all known IMINT activity. Compile from IMINT situation overall, pattern and analysis chart, and other CI products.

   d. (U) OTHER: Summarize any other pertinent enemy activity not already addressed.

2. (U) Counterintelligence Damage Assessment for the Period ___ to ___ (list DTGs)

   a. (U) Briefly assess the CI damage to MAGTF units for whom the assessment is being prepared. Assessment is based upon enemy intelligence and reconnaissance activities that were identified, analyzed, and reported, measured against the MAGTF operations profile and countermeasures implemented. Coordination with G-3/S-3 OPSEC/force protection staff is essential when preparing this paragraph.

3. (U) Estimated Enemy Activity for the Period ___ to ___ (list DTGs)

   a. (U) HUMINT: briefly describe estimated enemy HUMINT activity for the reporting period.

   b. (U) SIGINT: briefly describe estimated enemy SIGINT activity for the reporting period.

   c. (U) IMINT: briefly describe estimated enemy IMINT activity for the reporting period.

   d. (U) OTHER: briefly describe any other pertinent estimated enemy activity not addressed above.

4. (U) Counterintelligence Target Nominations

   a. (U) EXPLOITATION: identify any CI targets worthy of exploitation. Provide recommended timeframe, methods of exploitation, location, justification, and any other pertinent information.

   b. (U) NEUTRALIZATION: identify any CI targets worthy of nertralization. Provide recommended timeframes, methods of neutralization, locations, justifications, and any other pertinent information.

   c. (U) DESTRUCTION: identify any CI targets worthy of destruction. Provide recommended timeframe, methods of engagement, locations, justifications, and any other pertinent information.

- Identify necessary restrictions on informing MAGTF personnel about mission details, D-day, H-hour, designated landing beaches, helicopter landing zones, selected objective and other critical friendly force information requirements.
- Coordinate with the G-6/S-6 and subordinate commanders, and provide assistance with MAGTF communications and information systems security.

Support to Targeting

Supervise the accomplishment of CI operations in accordance with the CI plan. Including—

- Exploit sources of information to provide critical intelligence to commanders and planners. Provide pre-targeting surveillance and route reconnaissance enabling the commander to determine the appropriate method and force to be applied against the target.
- Assist with identifying MAGTF security and target vulnerabilities, evaluating the relative importance of each (MAGTF targets may be personalities, organizations, installations or capabilities). Additionally, identify security vulnerabilities of nongovernmental organization, private volunteer organizations, media, and other such organizations that are within the MAGTF's AO.
- Locate and recover contraband materials, such as arms, explosives, communication equipment, food, medical supplies, or other items not surrendered in accordance with proclamations. This denies critical capabilities to adversaries.
- Seize, exploit, and protect CI targets.

Combat Assessment

Continue an aggressive CI/HUMINT collection program in response to the MAGTF PIRs and IRs and in protection of MAGTF EEFIs to gauge the impact of friendly actions on the enemy and civilian populace and to evaluate the effectiveness of MAGTF security countermeasures.

6005. CI PLANS AND ORDERS

General

See appendix F for a list of MAGTF CI planning actions associated with each step of the MCPP.

Guidance for the conduct of MAGTF CI operations comes from many sources. The DIA 58 series of manuals and JP 2-01.2, are the principal references for U.S. CI operations and contains policy, direction, guidance, and instruction on how to perform the CI operations, activities and functions in compliance with national directives and security requirements (see appendix H for a detailed listing of CI and related references). Additionally, since MAGTFs will normally be part of a JTF or naval expeditionary force, reference to pertinent combatant command, JTF and fleet orders, guidance, and CI TTPs are necessary to identify unique operating concepts and methodologies and support procedures and formats. MAGTF CI plans and orders are prepared by the G-2/S-2. Plans developed by the G-2 plans officer

The G-2 plans officer coordinates the overall initial CI planning effort with the assistance of the ISC, CIHO, and the CO/OICs of organic and supporting CI units.

will then transition to the ISC, who is then responsible for detailed development of CI plans, their integration with other MAGTF intelligence, operations, CIS and logistics plans, and then principal oversight of execution. MAGTF CI plans and orders appear as an appendix to the intelligence annex of the MAGTF operation plan or order and will focus on internal MAGTF CI requirements, operations and TTP.

The CI Appendix

The CI appendix to an operations plan OPLAN or OPORD will be prepared consistent with format outlined in the Joint Operational Planning and Execution System (JOPES) and appear as appendix 3 (CI Operations) to Annex B (Intelligence) in all operations plans and orders. (See appendix B for a sample CI appendix format.) The CI appendix should include—

- Friendly forces to be used including—
  - Personnel augmentation requirements.
  - CI units of adjacent or other theater forces and the support expected.
  - Joint force maritime component commander (JFMCC) and ATF CI elements that may provide support to the landing force in amphibious operations.
  - Pertinent CI capabilities and support from the combatant command's joint intelligence center/joint analysis center, JTF joint Force J-2 (HUMINT staff element (J-2X), joint force land component commander, joint force air component commander, and other component commanders/task forces within JTF operations.
- Planned arrangement, employment, and use of external CI support including any special collection, production, dissemination, and CIS arrangements.
- Coordinating instructions established for the planning and control of CI operations including technical support expected from higher headquarters.
- MAGTF CI elements tasking.
- CI production priorities and plans.
- CI dissemination priorities and plans, including communication and information systems support to the MAGTF CI effort.
- CI unique equipment and logistics requirements.
- An appendix providing MAGTF countersigns, challenges, passwords, and supporting procedures.